نشاطات

مؤتمر (GISEC Global 2025) العالمي للأمن السيبراني لبنان بأمنيّه العام والداخلي ثانيًا بين 130 دولة

في 6 و7 و8 ايار الفائت، عقد في دبي معرض ومؤتمر الخليج لأمن المعلومات (GISEC Global 2025)، ثالث اكبر فعالية للامن السيبراني على مستوى العالم والاكبر في منطقة الشرق الاوسط وشمال افريقيا. شارك فيه اكثر من 750 شركة امن سيبراني في العالم كشركات (SANS) و(450)، Microsoft، ووفود زائرة من اكثر من 160 دولة

تضمن معرض ومؤتمر الخليج لأمن المعلومات، الذي انعقد تحت شعار "تأمين مستقبل مدعوم بالذكاء الاصطناعي"، تنظيم مسابقة عالمية في الامن السيبراني (Cyber Drill Global 2025)، شاركت فيها 130 فرقة استجابة للامن السيبراني من 130 دولة، من ضمنهم الوفد اللبناني المؤلف من ضابطين هما النقيب في المديرية العامة للامن العام علي الازوّر، والرائد في المديرية العامة لقوى الامن الداخلي جان بول شيبان اللذان فازا بالمرتبة الثانية بين 130 دولة مشاركة.

■ كيف تم اختيارك للمشاركة في معرض ومؤتمر GISEC Global 2025 في دبي؟

□ في الاساس، كل دولة تصلها دعوة لحضور المعرض والمؤتمر، تختار من ضمن فريق الاستجابة للهجمات السيبرانية لديها وفد لكي يمثلها. في لبنان ليس عندنا ما يسمى فرق استجابة للهجمات السيبرانية، وانما عندنا الهيئة الوطنية للامن السيبراني التابعة لمجلس الوزراء، والمديرية العامة للامن العام هي عضو فاعل في هذه الهيئة. الدعوة لمشاركة لبنان وجهت اساسا الى الهيئة الوطنية للامن السيبراني، والهيئة هي التي اختارتني من المديرية العامة للامن العام، واختارت الرائد في المديرية العامة لقوى الامن الداخلي جان بول شيبان كي يمثل الدولة اللبنانية في معرض ومؤتمر (GISEC Global 2025).

■ ما ابرز اهداف هذا المعرض - المؤتمر واي شركات عالمية شاركت فيه؟

□ يعد معرض ومؤتمر الخليج لأمن المعلومات من اهم معارض الامن السيبراني والذكاء الاصطناعي التي تقام في العالم، حيث تعرض فيه الدول والشركات المشاركة احدث اختراعاتها في تلك المجالات. كما يتم عقد محاضرات وندوات وحلقات حوارية تهدف الى تبادل الخبرات والاضاءة على اهم التحديات العالمية. لقد شاركت اهم الشركات العالمية في مجالي الامن السيبراني والذكاء الاصطناعي، ابرزها (SANS)، مايكروسوفت، غوغل كلاود للامن السيبراني، أمازون ويب سيرفسير، هواوي، وسيسكو. تخلل المعرض اجراء مسابقة Cyber Drill Global 2025 في الامن السيبراني التي نظمت من مجلس الامن السيبراني الاماراتي International Telecommunication Union – ITU، تبارت فيها 130 دولة، حيث فزنا بالمرتبة الثانية، وحصلنا على تهنئة خاصة من مجلس الامن السيبراني الاماراتي وITU.

■ عن اية عناوين عريضة تمحورت المسابقة؟

□ امتدت مسابقة Cyber Drill Global 2025، على مدى يومي 7 و8 ايار. تمحورت على 4 سيناريوهات مفصلة لمحاكاة حوادث الامن السيبراني الواقعية، حيث تم تصميم كل سيناريو لتعزيز المهارات التحليلية عبر مجالات مختلفة، بما في ذلك اكتشاف اختراق APT، تحقيقات OSINT، تتبع حملات التصيد الاحتيالي، وتحليل برامج الفدية. قدم كل سيناريو سياقا فريدا يتطلب عمليات صيد التهديدات، تحليل السجلات، الهندسة العكسية، التحليل الجنائي الرقمي، جمع المعلومات الاستخبارية من المصادر المفتوحة للكشف عن تكتيكات الخصوم، تحديد مؤشرات الاختراق (IOCs)، واقتراح الاجراءات الدفاعية المناسبة. في اليوم الاول تم اجراء اختبارين، وكذلك في اليوم الثاني.

■ هل يمكن تعريفنا على العناوين العريضة لكل من تلك الاختبارات الاربعة؟

□ في ما خص الاختبار الاول، تمحور على اكتشاف وتحقيق في اختراق (APT Advanced Persistent Threat). يحاكي هذا الاختبار هجوما مستمرا ومتطورا (APT) يبدأ باختراق جهاز واحد، ثم يتم الانتقال الافقي عبر الشبكة وصولا الى استخراج البيانات. يجري تقديم السجلات عبر منصة Malcom، بينما يتم مراقبة حركة الشبكة عبر Elasticsearch. يطلب من المشاركين الاجابة عن اسئلة تتعلق بـ:

- الادلة الرئيسية والعلامات (Flags).
- التكتيكات والتقنيات والاجراءات (TTPs) التي استخدمها المهاجم.
- خادم القيادة والسيطرة (C2).
- الادوات والاساليب المستخدمة في الهجوم.

■ ماذا عن الاختبار الثاني؟

□ تمحور الاختبار الثاني على تحقيق OSINT في الانترنت المظلم حيال هجوم ارهابي الكتروني. في هذا الاختبار، تم تقديم صورة لمحطة 5G مخربة تحمل شعار "اوقفوا 5G وكونوا احرارا"، ومستند PDF يصف الحالة، منشورات على Facebook، ورسالة بريد الكتروني ارسلت عبر ProtonMail تشير الى الحملة نفسها. يطلب من المشاركين اجراء تحقيق استخباراتي مفتوح المصدر (OSINT) للكشف عن جميع المحتويات ذات الصلة وجمع نحو 30 علامة مرتبطة بالحالة، بما في ذلك تتبع البصمات الرقمية، واكتشاف المجتمعات عبر الانترنت، وتحديد الجهات الفاعلة.

النقيب في المديرية العامة للامن العام علي الازوّر.

■ بالنسبة الى اليوم الثاني من المسابقة، على ماذا تمحور اول اختبار فيها؟

□ حول محاكاة لحملة تصيد احتيالي تستهدف مؤسسة مالية، بحيث يجب على المحققين القيام بالآتي:

- تتبع مصدر رسائل التصيد الاحتيالي وتحديد نقطة الدخول الاولية.
- تحليل مضيف الشبكة والبيانات لتتبع تقدم الهجوم.
- تحديد اي اليات للبقاء وكيفية جمع بيانات الاعتماد.
- ربط سلوك المهاجم بتقنيات MITRE ATT&CK.
- اعداد تقرير شامل عن الحادث يتضمن IOCs، تأثير الهجوم، والتوصيات المناسبة للتنسيق مع وكالات انفاذ القانون.

■ ماذا عن الاختبار الرابع والاخير؟

□ تركز على تحليل برامج الفدية (Ransomware) وفك التشفير. هذا الاختبار يتضمن جهازا مصابا ببرامج ضارة تحتوي على اداة اسقاط (Dropper) ومكون لبرنامج الفدية. يتم عزل النظام المصاب، ويطلب من المشاركين اجراء تحليل جنائي كامل:

- تحديد نقطة الاختراق الاولية.
- فحص الاحداث النظامية لاكتشاف وجود البرامج الضارة.
- كشف آليات البقاء التي استخدمها المهاجم.
- اجراء الهندسة العكسية لأداة الاسقاط لاستخراج IOCs واكتشاف تحميل البرمجية الثانية المشفرة.
- فك تشفير وتحليل البرمجية الثانية لاسترجاع مفتاح فك التشفير.
- استعادة الملفات المشفرة باستخدام المفتاح المستخرج.

المسابقة تضمنت 4 اختبارات مكثفة على مدى يومين

■ ما اهمية دور الذكاء الاصطناعي في مختلف مجالات الامن السيبراني؟

□ كل التقنيات السيبرانية الحديثة اصبحت مدمجة بالذكاء الاصطناعي، اي هو جزء اساسي ومحوري ضمنها. كما ان برامج الذكاء الاصطناعي اصبحت قادرة على التحليل وادارة الهجمات السيبرانية بمفردها. كما يقوم البرنامج بتحليل بيانات الشبكة والتنبؤ بافضل الاوقات والاساليب لتنفيذ هجوم ناجح. وعندما يجد ان التوقيت مناسب، ينفذ الهجوم تلقائيا بحسب افضل طريقة يجد انها الانسب، وكذلك يتعاطى مع اي مستجدات تطرأ بحسب ما يراه مناسبا من كل النواحي التقنية والنفسية. هنا، يجب التأكيد على ان للذكاء الاصطناعي وجهين، الاول مفيد عند استخدامه لمكافحة الجرائم وحماية المجتمع، والثاني سيئ جدا عند استخدامه من مجرمين وشبكات الاجرام المنظم في تنفيذ جرائمهم، حيث يشكل خطرا كبيرا على المجتمع.

■ في ظل هذا التطور التقني، كيف يستطيع المواطن العادي ان يحمي نفسه من الجرائم السيبرانية؟

□ امام هذا التطور التكنولوجي الهائل في العالم، وفي ظل حقيقة مفادها ان الجرائم السيبرانية قد تطال المواطن عبر هاتفه الخلوي او حاسوبه الشخصي، داخل منزله او في عمله، حيث لا وجود للشرطة ولا يعلم بها احد سواه، فان احدى اهم وسائل الحماية هي توعية المواطنين وتثقيفهم في المجال السيبراني. على هذا الاساس، ان المديرية العامة للامن العام، في موازاة كل الجهود الامنية الجبارة التي تقوم بها على كل الصعد، اطلقت عام 2019 حملة توعية على مخاطر الفضاء السيبراني تحت شعار "حتى ما تكون ضحية". بناء عليه، ومنذ ذلك الحين، يقوم ضباط من المديرية بإلقاء محاضرات في المدارس والجامعات والنوادي الاجتماعية على امتداد مساحة الوطن بهدف توعية الطلاب والطواقم التعليمية والاهالي على المخاطر والجرائم السيبرانية وطرق وتقنيات الحماية منها، اضافة الى سواها من الاجراءات المشابهة. بالتالي، ان المديرية العامة للامن العام تبذل اقصى جهودها في كل المجالات الأمنية والتقنية والتوعوية من اجل حماية المواطن الذي هو رب عملنا وكل امكاناتنا في خدمته كما يؤكد دائما المدير العام للامن العام اللواء حسن شقير في لقاءاته مع العسكريين والاعلاميين.