مقابلة

تريز الخوري
khourytherese@hotmail.com

# الحماية الإلكترونيّة هي الأسلم ضدّ الهجمات الحاسوبيّة أبوذياب: صون المعلومات أصبح حتمياً للإستقرار والأمان

**تعد المحاضرات المتخصصة في الامن السيبراني ضمن الامن العام امرا ضروريا لمواجهة التهديدات الافتراضية المتزايدة. مع تنوع اساليب الهجمات الرقمية وتطورها، يصبح تدريب العاملين في هذا المجال على حماية البيانات وتعزيز المهارات التقنية، مسألة جوهرية لضمان سلامة المحتوى وحمايته من المخاطر التي قد تهدد استقرار المجتمع وتخلق تحديات كبيرة ومعقدة**

في قلب هذا المشهد الرقمي المعقد، تتنوع التهديدات السيبرانية في طبيعتها واساليبها واهدافها، مما يجعل مواجهتها اكثر صعوبة. فقد تطورت من مجرد فيروسات عشوائية ترسل عبر البريد الالكتروني الى هجمات دقيقة وموجهة، تعتمد على التحليل العميق لأنظمة الضحية، وتنفذ باستخدام تقنيات معقدة من الهندسة الاجتماعية والتلاعب بالسلوك البشري، وصولا الى اعتماد الذكاء الاصطناعي في تطوير البرمجيات الخبيثة. من اخطرها، تلك التي تشفر فيها بيانات المستخدم او المؤسسة، وتحتجز رهينة حتى يتم دفع مبلغ مالي. وقد استهدفت المستشفيات والمطارات والمؤسسات الحيوية، مما تسبب في تعطيل خدمات عامة وشلل اداري تام. الى ذلك، هناك التصيد الاحتيالي، وهو غالبا ما يصل في شكل رسائل او مواقع الكترونية مزيفة تهدف الى الخداع وسرقة البيانات الشخصية او المصرفية. اما الهندسة الاجتماعية، فتعتمد على استغلال العامل البشري نفسه باعتباره الحلقة الاضعف، من خلال التلاعب بعواطف او السلوكيات لاقناعه بالكشف عن معلومات سرية، او النقر على روابط خطيرة.

في هذا السياق، ظهرت اخيرا غزوات اكثر تطورا تعرف بالمتقدمة المستمرة (APT)، تستهدف عادة الحكومة او شركات كبرى، حيث يخترق النظام بهدوء ويظل في داخله لفترات طويلة. وهي لا تقتصر على المجال التقني وحده، بل لها ابعاد امنية واقتصادية وسياسية. ففي بعض الحالات، تم استخدام الهجمات كأداة في الحروب بين الدول عبر استهداف شبكات الكهرباء او وسائل الاعلام او حتى الانتخابات. في اطر اخرى، ساهمت في انهيار سمعة شركات كبرى وفقدان ثقة العملاء والمستثمرين بها، ما ينعكس سلبا على الاقتصاد. هذا التنوع في التهديدات وتداخلها يجعل من الامن السيبراني ساحة معركة دائمة التطور، تتطلب يقظة عالية وتحديثا مستمرا للانظمة، إضافة الى تعاون فعال بين مختلف الاطراف، من جهات حكومية ومؤسسات خاصة، وصولا الى المستخدمين الافراد الذين باتوا جزءا اساسيا من منظومة الحماية او مصدرا محتملا للثغر.

"الامن العام" حاورت الملازم في دائرة الاتصالات في الامن العام دينا ابوذياب التي قدمت من خلال محاضرة القتها في المديرية العامة للامن العام عرضا مفصلا للجوانب التقنية والقانونية المتعلقة بحماية الشبكات، حيث تناولت العوائق التي تهدد المجتمع، وناقشت سبل الحد منها والتعامل معها. كما شرحت كيفية تمكين الشخص من حفظ نفسه عبر تقنيات معينة، واختتمت بالاشارة الى ضرورة التواصل مع الجهات المعنية في حال التعرض لأي تهديد او ابتزاز، مشددة على اهمية الحفاظ على سرية المعلومات.

■ ما هو تعريف الامن السيبراني، ولماذا حظي بكل هذا الاهتمام اخيرا؟

□ لم يعد الامن السيبراني مجرد مصطلح فني نسمع عنه في المؤتمرات او ندوات التكنولوجيا، بل اصبح جزءا اساسيا من بنية المجتمعات الحديثة. في اختصار، هو علم حماية الانظمة الالكترونية والشبكات والبيانات من اي اعتداءات او اختراقات او استغلال. هذا يعني ان تكون بياناتك الشخصية ومعلوماتك البنكية واسرار المؤسسات التي تعمل فيها او تتعامل معها، محمية من عبث القراصنة او تسريبها بطرق غير مشروعة، كوننا اصبحنا نعيش حياتنا بشكل شبه كامل في الفضاء الرقمي، من التعليم والعمل وحتى الطب والتسوق والتواصل الاجتماعي. التكنولوجيا اصبحت في صلب اهتمامنا، وتاليا اي خلل او اختراق قد تكون له عواقب كارثية، ليس فقط على الافراد بل على الدول ايضا. الاحداث الاخيرة اثبتت ان الحروب لم تعد تخاض فقط على الارض، بل هناك جبهات رقمية لا تقل ضراوة عن المعارك العسكرية.

■ ما هي طبيعة التهديدات السيبرانية حاليا، ومن هي الجهات الاكثر عرضة للاستهداف؟

□ الامور لم تعد تقتصر على هاكرز مراهقين يجربون مهاراتهم. نحن نتحدث اليوم عن عصابات منظمة عابرة للحدود، وعن كيانات مدعومة من دول تمتلك موارد هائلة واهدافا استراتيجية واضحة. الادوات المستخدمة تتراوح بين برمجيات الفدية، الى التصيد الاحتيالي الذي يستهدف الافراد للحصول على بياناتهم البنكية او كلمات المرور، الى ما يعرف بـ"الهندسة الاجتماعية" التي تعتمد على خداع الناس للحصول على معلومات حساسة. اما الجهات المستهدفة، فهي متنوعة جدا. المؤسسات المالية كانت تاريخيا الهدف الاول، لكننا نلاحظ اليوم توسعا كبيرا في دائرة الهجوم التي باتت تشمل جميع المؤسسات وصولا الى البلديات والادارات العامة. السبب بسيط: يركز القراصنة على الاماكن التي تحدث فيها الفوضى اقصى قدر من الاذى، فتجبر تاليا على الدفع او التنازل بسرعة.



الملازم في دائرة الاتصالات في الامن العام دينا ابوذياب.

■ كيف يمكن للدول ان تبني استراتيجيا وطنية فعالة للحد من الاختراقات؟

□ يجب ان يكون هناك وعي على مستوى القيادة السياسية بأن هذا الملف هو اولوية وطنية، تماما كالدفاع العسكري. فالخطوة الاولى في بناء استراتيجيا وطنية ترتكز على وجود خطة مركزية مسؤولة عن تنسيق الجهود وتوحيد المعايير، لذا يجب انشاء مراكز للاستجابة للطوارئ، وتفعيل آليات الرصد المبكر، وبناء قاعدة بيانات وطنية لمتابعة الحوادث والهجمات وتحليلها. من الضروري ايضا اشراك القطاع الخاص في هذه المعركة. ان غالبية البنى التحتية التكنولوجية في الدول الحديثة مملوكة او مشغلة من شركات خاصة، لذلك لا يمكن تحقيق امن فعال من دون تعاون وثيق معها. هنا نحتاج الى قوانين تلزم هذه المؤسسات بمستويات معينة من الحماية، وتبليغ الجهات المختصة في حال حدوث خرق.

■ في ظل تطور تقنيات الذكاء الاصطناعي، هل يمثل هذا التقدم فرصة ام تهديدا جديدا؟

**نستطيع الحفاظ على سرية المعلومات لمنع حدوث انتهاكات**

□ الذكاء الاصطناعي سلاح ذو حدين بامتياز. من جهة هو اداة قوية جدا لمكافحة الهجمات، لأنه يمكن ان يتعلم من الانماط ويكتشف السلوكيات المشبوهة بشكل اسرع من البشر، ويمكنه تحليل كميات ضخمة من البيانات في وقت قصير، مما يسمح برصد التهديدات في مراحلها الاولى. لكن من جهة اخرى، يمكن للقراصنة انفسهم استخدامه لتطوير هجمات اكثر تعقيدا، ولتجاوز انظمة الحماية التقليدية. الاسوأ من ذلك، ان هناك برمجيات هجومية باتت تباع على الشبكة المظلمة، وتستخدم تقنيات "التعلم الالي" لتكييف سلوكها مع ظروف النظام المستهدف. السباق الان هو بين من يطور ادوات اسرع واكثر فاعلية: المدافعون ام المهاجمون؟

■ في ظل كل هذه المخاطر كيف يمكن للافراد حماية انفسهم؟ هل هناك خطوات بسيطة يجب الالتزام بها؟

□ معظم الهجمات الالكترونية الناجحة تبدأ من خطأ بشري بسيط: رابط تم النقر عليه، او كلمة سر تم استخدامها في اكثر من مكان، او شبكة واي فاي عامة تم الاتصال بها من دون حماية. على كل فرد ان يعتبر نفسه بوابة يمكن ان تؤدي الى اختراق اكبر. لذا يجب استخدام كلمات مرور قوية وفريدة، تفعيل المصادقة الثنائية، تحديث الاجهزة والبرامج باستمرار، عدم مشاركة المعلومات عبر وسائل غير آمنة، كلها اجراءات بسيطة لكنها مفيدة. لكن الاهم من كل ذلك، هو التوعية. يجب ان نغرس في الجيل الجديد ثقافة امن المعلومات منذ المراحل الدراسية الاولى، تماما كما نعلمهم السلامة المرورية او قواعد النظافة.

■ ما الهدف من اجراء محاضرات تدريبية للامن العام؟

□ كل ما نقوم به يهدف الى تأهيل قدرات الافراد وتعزيزها، والعمل على رفع مستوى الوعي حول المخاطر الرقمية وسبل الوقاية منها. فمن خلال ذلك، يصبح من الممكن التعرف على التهديدات والتعامل معها قبل ان تؤثر على البنى التحتية. في سياق آخر، ان عملنا يرتكز على المهارات اللازمة للتعامل مع الانظمة الامنية المتطورة لمنع اي اختراق او تسلل مهما كان نوعه، مما يعزز القدرة على تطبيق تقنيات متقدمة للحفاظ على سلامة الشبكات. كما نوجه المتدربين على حماية المعلومات المهمة والحد من الاضرار الناجمة عنها. كذلك نساهم في بناء قدرة المؤسسة على التصدي بشكل احترافي، مما يساعد في الحفاظ على المواطنين والمؤسسات الحيوية.

■ على ماذا تركزين في عرضك المسهب عن مخاطر الاختراق؟

□ مجموعة من المواضيع الاساسية التي ◄

◄ تهدف الى حث المشاركين على التصدي للتهديدات الرقمية، وقد تم تقديم نظرة شاملة عن المفاهيم الرئيسية في الامن السيبراني، بما في ذلك انواع الهجمات. في هذا الاطار، شددت على افضل الممارسات لحماية الشبكات والبيانات، على ان يكون ذلك في تقوية كلمات المرور، تحديث الانظمة، وكيفية التعامل مع الثغر الامنية. كما تطرقت ايضا الى الاستجابة للطوارئ بما في ذلك كيفية التصرف عند وقوع الهجوم المفاجئ.

■ كيف يمكن للامن العام المحافظة على سرية بياناته؟

□ الحفاظ على سرية المعلومات يعتبر من الاسس الجوهرية التي نعتمد عليها في اداء مهامنا بشكل فعال وآمن. لضمان حماية معلوماتنا من التسريب او الاستغلال غير المشروع، نتبع مجموعة من الاجراءات التقنية والقانونية والادارية المتكاملة:
اولا، نعتمد على التشفير القوي للبيانات والانظمة.
ثانيا، يتم تطبيق اجراءات رقابة داخلية صارمة بدءا من تحديد صلاحيات الوصول الى المعلومات بناء على الحاجة والاختصاص.
ثالثا، نقوم بتدريبات مستمرة للموظفين والمتعاملين مع المعلومات الدقيقة، بحيث يتلقون افضل الممارسات للحماية.
كما يشمل عملنا كيفية التعرف على المخاطر المحتملة، مما يساعد في الحفاظ على مستوى عال من الوعي حول كيفية حماية البيانات.
اخيرا، نلتزم اجراءات صارمة لضمان حماية الخصوصية من الاختراق.

■ ما هي نصيحتك الى ضباط الامن العام ومفتشيه؟

□ في العصر الرقمي الذي نعيش فيه، لم تعد السرية شخصية فحسب، بل اصبحت جزءا من مسؤولياتهم الامنية اليومية. فمع ازدياد حجم التهديدات السيبرانية وتعقيد اساليب الهجمات، بات من الضروري التعامل مع الاستقلالية على انها خط الدفاع الاول في مواجهة محاولات الاختراق والتجسس والاستهداف المباشر. ينبغي على كل عنصر امني ان يتبنى ممارسات رقمية آمنة تبدأ من اختيار كلمات مرور قوية وفريدة، واستخدام تقنيات التوثيق المتعدد، وصولا الى وعي المخاطر المترتبة على مشاركة المعلومات عبر الانترنت، حتى تلك التي تبدو عادية او غير حساسة. ما اود توضيحه هو ان الكثير من الهجمات تبدأ من استغلال معطيات بسيطة تنشر في مكان غير مناسب. كما ان اعتماد الاجهزة الالكترونية يجب ان يكون تحت مراقبة دائمة مع تحديثات منتظمة للبرامج، وتثبيت الحماية المتقدمة خاصة على الهواتف الذكية واجهزة الكومبيوتر التي تستخدم احيانا في العمل. فالمخاطر لا تأتي فقط من الخارج، بل قد تنشأ من ثغر صغيرة في الاجهزة المستخدمة يوميا. الوعي على كيفية التصرف عند مواجهة تهديد كرسالة مشبوهة او محاولة اختراق، يجب ان يكون حاضرا دائما. فالمعرفة المسبقة تجنب الوقوع في الفخ، وتمنح القدرة على التحرك السريع لحماية الذات والمؤسسة. هنا تبرز اهمية المشاركة في الدورات التدريبية الامنية بشكل مستمر، لأنها تتيح تحديث المعارف وتعزيز المهارات في التصدي للهجمات الرقمية الحديثة. اضافة الى ذلك، لا بد من الحذر الشديد عند استخدام الشبكات العامة او مشاركة الملفات والبيانات خارج الاطار الآمن. فالعالم الرقمي مليء بالفخاخ التي لا تشاهد بالعين المجردة، وقد تكون بوابة لتهديد اكبر. مسؤولية كل ضابط او مفتش يجب ان لا تتوقف عند حماية نفسه فقط، بل تمتد الى حماية المؤسسة التي يمثلها والمعلومات التي يتعامل معها، والتي قد تشكل في حال اختراقها خطرا مباشرا على الامن القومي. لذا فان اليقظة والتصرف الواعي والالتزام بالتدابير الوقائية ليست مجرد توصيات، بل ضرورات لحماية الذات والمحيط. اخيرا التعامل الذكي ينعكس مباشرة على كفاية العمل الامني، ويعزز مناعة المؤسسة في وجه اي اختراق محتمل. الخصوصية ليست رفاهية، بل صراع اساسي ومتواصل مع تهديدات لا تنام.

**الامن العام يعتمد افضل وانجح الممارسات لحماية البيانات**

من المحاضرة.