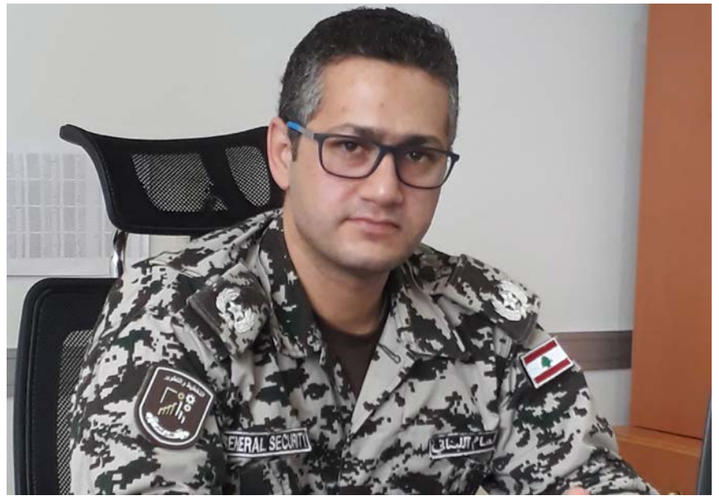
تحقيق

خليل حرب
khalilharb66@gmail.com

ورش عمل برعاية الأمن العام لوضع استراتيجيا فعّالة

تكنولوجيا المعلومات: أخطار خفيّة في موازاة التطور

لبنان في سباق مع الزمن. اذا تأخر او تعثر في ظل التطور المتسارع في مجال تكنولوجيا المعلومات، انكشفت دفاعاته امام الغزو السيبراني الذي يستهدفه، ليصبح اكثر عرضة لتهديدات باتت تشكل خطرا عالميا على الصعيد الامني والاجتماعي والاقتصادي من خلال هجمات الكترونية تنفذ خلال ثوان. ثمة حركة فاعلة في لبنان للوقاية، تشارك المديرية العامة للامن العام فيها بفاعلية، لمواجهة المخاطر التي تلوح امامه يوميا



رئيس دائرة ادارة الجودة في الامن العام الرائد الاداري احمد فواز.

لنتفق اولا على ان المعلومات على اختلاف انواعها، والتي باتت تشكل احد اهم واخطر اصول الشركات والمؤسسات العامة والخاصة وحتى الاشخاص، تحتاج الى حماية، سواء كانت ورقية كما في الملفات المحفوظة في الارشيف التقليدي، او الكترونية مثلما اصبح حال غالبية معلوماتنا في عصرنا الحالي في ظل تطور تكنولوجيا المعلومات واساليب التخزين الرقمية لها، سواء كانت معلوماتنا الشخصية او الامنية او المالية او المصرفية وغيرها.

كذلك الامر فان الاعمال اليومية والعمليات التشغيلية للشركات والاشخاص باتت تعتمد بشكل اساسي على الانترنت وتكنولوجيا المعلومات. وهنا يأتي دور الامن السيبراني ليعنى بحماية هذه المعلومات والاعمال.

> **الامن العام مؤتمن على كل معلومة في حوزته**
>
> **الخطر مصدره افراد او عصابات او اجهزة استخباراتية**

ثمة حروب الكترونية دائرة على مستوى العالم وداخل كل دولة. هناك قراصنة (هاكرز) على مستوى الافراد، العصابات، او الجريمة المنظمة، او الهيئات التابعة لدول وحكومات، تعمل ليل نهار من اجل اهداف عدة، من بينها النيل من المعلومات الشخصية للافراد او الجماعات، او محاولة اختراق الانظمة المشغلة لكل الخدمات الاساسية للدول كالشبكات الكهربائية وخطوط الطيران الجوي والنقل البحري ونظم المياه والقطاع المصرفي ودوائر الامن، او ارسال فيروسات الكترونية للسطو على بياناتها او تعطيلها او تخريبها بالكامل.

الاهداف متعددة، من بينها الابتزاز المالي او السياسي او الاقتصادي، او ممارسة فعل عدائي بهدف التدمير او التخريب، او التجسس على الدول والشركات والافراد.

تتجسد هذه الحقائق فيما لبنان يحتل المرتبة 119 من بين 165 دولة من دول اعضاء الاتحاد الدولي للاتصالات، وفق تقرير مؤشر قياس استعداد الدول في مجال الامن السيبراني لعام 2017.

يقول رئيس دائرة ادارة الجودة وضابط اتصال مشروع الادارة المتكاملة للحدود في المديرية العامة للامن العام الرائد الاداري احمد فواز ان "المعلومات تشكل احد اهم اصول المؤسسة او المنظمة او الحكومة وهي ضرورية لعملها. لهذا تتحتم حمايتها في هذا الفضاء السيبراني الواسع حيث تتقدم التكنولوجيا بشكل مستمر ومتسارع، وصار الاختراق او السطو على هذه المعلومات لشخص او مؤسسة، يشكل جريمة موصوفة".

ويوضح الرائد فواز ان "مصادر الخطر يمكن ان تأتي من افراد او عصابات او منظمات اجرامية او اجهزة استخباراتية لتحقيق احد هذه الاهداف او البعض منها:

الخبير في المركز الدولي لتطوير سياسات الهجرة باول وزنياك.

اشهر القراصنة وأهم الاختراقات

لعل عملية "كاربانك سايبرغانغ" من اشهر الاختراقات للامن السيبراني، اذ استغرق الاعداد لها نحو عامين وشملت 30 دولة بينها روسيا والولايات المتحدة واليابان وسويسرا ونحو 100 مصرف. بلغت حصيلتها مليار دولار، وتمت في العام 2015 عبر رسائل الاحتيال في البريد الالكتروني للمصارف.

وفق احد الخبراء، فان القراصنة اخترقوا الكومبيوترات واحدا تلو الاخر، وكانوا يرسلون الاموال الى اجهزة الصراف الالي في وقت محدد، فتخرج منها بشكل اوتوماتيكي ويتسلمها احد شركائهم فورا.

في حزيران عام 2015، اعلنت الحكومة الاميركية ان قراصنة تمكنوا من سرقة بيانات قرابة اربعة ملايين موظف فيديرالي، بينهم عملاء لاجهزة الاستخبارات الاميركية. اتهمت الصين بالضلوع في الهجوم الاكبر في تاريخ الولايات المتحدة.

قبل اكثر من ثلاثة اعوام، اعلنت مجموعة تسمي نفسها "شادو بروكرز" اختراق وكالة الامن القومي الاميركي، والحصول على انظمة اختراق وقرصنة الكترونية، وما سموه اسلحة سايبرية تتضمن برامج تشغيل استخدمتها الولايات المتحدة في تخريب البرنامج النووي الايراني، وعرضوا ما في حوزتهم للبيع في مقابل 580 مليون دولار.

اما مجموعة "غلوبال هيل" فانها مسؤولة عن تخريب موقع الجيش الاميركي على الانترنت، وتدمير المعطيات والمعلومات الخاصة بـ155 موقعا الكترونيا، اضافة الى تجارة المعلومات غير الشرعية، وتقدر الاضرار الناجمة من اعمالها بملايين الدولارات.

عصابة "تيمبويزون" نجحت في اختراق الموقع الرسمي لحلف شمال الاطلسي والفايسبوك، وفي سرقة المعلومات الشخصية لرئيس الوزراء البريطاني الاسبق طوني بلير من خلال اختراق بريده الالكتروني، اضافة الى الهجوم على شركة "ريسرش ان موشين" التي طورت هواتف بلاكبيري.

لكن مجموعة "انونيموس" لا تزال الاكثر شهرة في السنوات الاخيرة على مستوى العالم. فقد تكررت هجماتها على اسرائيل، كما هاجمت وزارة الدفاع الاميركية وهددت بتدمير الفايسبوك.

في مطلق الاحوال، يعتقد ان العام 2014 شهد اعلى مستوى من القرصنة، مع 81 مليون حادث الكتروني امني، منها 12 الف هجمة امنية تخريبية، واكثر من 100 حادث امني جرى التحقيق فيها بحسب شركة "آي بي ام".

من بين اشهر اسماء القراصنة على مستوى العالم: كيفن ميتنيك، كيفن بولسن، ادريان لامو، ستيفن وزنياك، ويد بلانكنشيب، مايكل كالي، روبرت تابان، موريس وسفين جاشان.

- عرقلة استمرارية النشاط الاقتصادي لدولة او مؤسسة.
- السطو على معلومات.
- التلاعب بالمعلومات (الداتا).
- اثارة خوف وفوضى عبر استهداف البنى التحتية لدولة.
- الحاق اذى مالي بشركة.
- نشر اخبار تمس المعتقدات الدينية او السياسية.
- تحقيق اهداف عسكرية معينة.
- انتقام من شخص او مؤسسة او جهة حكومية، او طلب فدية".

"البلد مفتوح على العالم السيبراني"، يقول الرائد فواز، في حين ان الهاكرز هم في حالة تطور مستمر، ومن يعملون على مقاومتهم (اشخاص، مؤسسات او اجهزة) هم في سباق دائم معهم ايضا، نظرا الى التطور المستمر لعلم الاختراق واساليبه، والحاجة المستمرة الى تحديث اساليب الدفاع.

من بين اخطر التحديات "صعوبة تحديد مواقع انطلاق الجريمة، لان الاختراق يمكن ان يتم من منزل، او مقهى، او شركة، او من داخل البلد او خارجه، ومن المؤسسة او خارجها، ما يعني ان الحدود الافتراضية لبلد معين والتي يتطلب حمايتها من الاختراق او الاستهداف، ربما تكون اكثر صعوبة وتحديا وخطرا من الحدود الجغرافية"، بحسب ما اشار اليه الرائد فواز.

يعطي مثالا عن المديرية العامة للامن العام "المؤتمنة على كل معلومة في حوزتها، والتي تملك مجالين لعملها، امني وخدماتي". ويشير الى ان "المخترقين قد يحاولون النيل من المعلومات الامنية والشخصية المتعلقة بالاشخاص او المؤسسات والتي يجب ان لا يطلع عليها سوى الاطراف المعنيين بها. في حين انه في الشق الخدماتي، فان المديرية العامة للامن العام، نظرا الى عملها في ادارة الحدود والمسافرين واصدار وثائق السفر او بطاقات الاقامة والتاشيرات والتصاريح وغيرها، في حوزتها معلومات شخصية وتفاصيل وعناوين وتواريخ حركة دخول وخروج، يمكن ان تكون هدفا لقراصنة يحملون نيات جرمية او استغلالية، بما يؤدي الى نتائج كارثية ◄

احدى ورش العمل.

على الناس من بينها ابتزازهم ومتابعتهم امنيا واستهدافهم، اي انها تشكل خطرا على حياتهم واموالهم. ناهيك بالخطر المتأتي من تسرب معلومات امنية متعلقة بالاشخاص، المؤسسات، او الدول، لصالح جهات ذات دوافع اجرامية.

يخلص فواز الى القول ان المديرية العامة للامن العام، كغيرها من المؤسسات، "لها شبكات داخلية للاتصال وشبكات مفتوحة على الفضاء السيبراني، ولهذا قد تكون عرضة لخطر التسلل الى شبكاتها وانظمتها".

من اجل ضمان توافر واستمرارية عمل نظم المعلومات وشبكاتها وتعزيز الحماية وسرية البيانات الشخصية وخصوصيتها وحماية المؤسسة والمواطنين من المخاطر في الفضاء السيبراني، قام المركز الدولي لتطوير سياسات الهجرة، في اطار مشاريع ممولة من الاتحاد الاوروبي، بالتعاون مع الامن العام، بتنظيم نشاطات وورش عمل في مجال الامن السيبراني، شملت ضباطا وعناصر من قطاعات متخصصة بتكنولوجيا المعلومات او امن الشبكات على المستوى التقني، اضافة الى ضباط قادة من جميع المكاتب، الى جانب دورات توعية لعسكريين من جميع قطاعات الامن العام لتعريفهم بالامن السيبراني والاخطار التي

> **السباق مستمر بين الهاكرز ومن يقاومهم**
>
> **لبنان مفتوح على العالم السيبراني**
>
> **استراتيجيا امن سيبراني للبنان هي الهدف المطلوب**

يمكن ان يواجهونها على المستويات الفردية والشخصية والعملية ضمن المؤسسة.

الخبير في المركز الدولي لتطوير سياسات الهجرة باول وزنياك الذي ساهم في ورش العمل والتدريب، اشار الى ان نشاطات المركز الدولي لتطوير سياسات الهجرة شملت ضباطا وعناصر من الامن العام والجيش والامن الداخلي والجمارك والدفاع المدني، مشيرا الى "اننا نعزز في الخطوات الاولى الوعي اولا بالامن السيبراني، بهدف الوصول الى استراتيجيا الامن السيبراني".

وبحسب وزنياك، فان ورش العمل خلال تشرين الثاني 2018 شملت قضايا عدة من بين عناوينها: المعلومات كقوة وامنها، اهداف ومخاطر مرتبطة بأمن المعلومات، العمل التنظيمي (الهيكلية والاجراءات والادوار والادوات)، الامن مسؤولية الجميع، التهديدات السيبرانية، الامن السيبراني في بولونيا وفي جهاز الشرطة تحديدا، تأمين الشبكات، العملات الرقمية (مثل البيتكوين)، امن اجهزة الهواتف، الشبكات المنزلية، البريد الالكتروني، والانظمة المصرفية.

يؤكد وزنياك ان المسألة "لم تعد ترفا، اذ ان 70% من عمليات الهاكرز تستهدف الناس العاديين لان عملياتهم عادة ما تكون اكثر سهولة". ويتحدث عن جهات في دول شديدة التطور في مجال القرصنة من بينها الصين، الولايات المتحدة، روسيا واسرائيل وايران. ويعتبر ان اي دولة في العالم معرضة لهجمات الهاكرز اذا اتخذ القرار.

ما من احد في مأمن، يقول وزنياك، "اذ لم يعد الامر متعلقا باجهزة الكومبيوتر الشخصية فقط، اذ ان هناك الهواتف الذكية، وهناك كومبيوترات تشغيل الاضاءة والانارة والحرارة والموسيقى في المنازل، كلها يمكن التسلل اليها ومنها الى خصوصيات الناس في بيوتهم او اماكن عملهم".

لهذا يعتبر الخبير الاوروبي ان الامر بات يتطلب تعاونا بين مختلف دوائر الدولة، وليس فقط اقسام تكنولوجيا المعلومات"IT" المتخصصة، لان الاهتمامات والمخاطر تتوسع وتشمل الجميع، اذ في امكان الهاكرز تنفيذ هجومه بما يعادل سرعة الضوء تقريبا من بلد يبعد عنا الاف الكيلومترات.

ويلفت الى ان "الاستعداد لهجوم الهاكرز قد يتطلب عامين احيانا، اما الهجوم نفسه فيمكن ان يتم خلال ثوان قليلة. احيانا، من خلال الامن السيبراني لمواجهة الهاكرز، قد نتمكن من تقليص خسائر جهة ما الى مئات الاف الدولارات بدلا من ملايين الدولارات، او قد نتمكن من انقاذ ارواح العديد من الناس اذا كان الهدف من الاختراق نشر شائعات واخبار مضللة للمواطنين في بلد ما".