عجز مدمّر في مواجهة الهجمات السيبرانية

مع توسّع الهجمات السيبرانية وانتشارها وتطوّر تقنياتها وأساليبها في العالم، باتت المخاطر الأمنيّة الإلكترونية تشكّل تهديداً كبيراً على جميع المستويات من أفراد إلى مؤسّسات وشركات، وحتّى دول. وفي لبنان، تظهر الأزمات المتتالية مكامن ضعف هائلة في العديد من مرافق الدولة على الصعيد التقني وفي ما يخصّ تكنولوجيا وأمن المعلومات، بسبب هشاشة البنية التحتيّة وسوء الإدارة وشحّ الموارد المالية، وفي أحيان كثيرة قلّة الخبرة التقنيّة وعدد العاملين في مجالات أمن المعلومات والبيانات. نعرض في ما يلي أمثلة حقيقية عن هجمات إلكترونية تعرّضت لها إدارة رسميّة (المديرية العامّة لوزارة الأشغال)، هي من جملة هجمات متعدّدة استهدفت مؤسّسات حكومية لبنانية ومواقع حيوية، ولا سيّما في ضوء الأزمة الرّاهنة، وكيفية تعامل هذه المؤسّسات والجهات الحكومية مع هذه الحوادث، وما هي الإجراءات المتّبعة ومن الضروريّ اتخاذها في مثل هذه الحالات؟

يصبح العالم مع مرور الوقت أكثر اعتماداً على شبكة الإنترنت، وبالتالي، بتنا عرضةً بشكل متزايد للهجمات السيبرانيّة. في السنوات الأخيرة، شهدنا أحداثاً هائلة وأزمات أجبرت الدّول والمؤسّسات والأفراد على دمج الفضاء الإلكتروني في الحياة العمليّة بشكل كبير، ولا سيّما خلال فترة انتشار جائحة «كورونا» وتكيّف الناس مع فكرة التواصل والعمل «أونلاين». ونظراً إلى أن البنية التحتيّة الأساسية ضرورية لعمل المؤسّسات والإدارات وبالتالي عمل المجتمع، غالباً ما تعدّ الأكثر استهدافاً بخاصة في أوقات الأزمات وأزمنة الحرب. تشمل هذه البنية التحتية عادةً أنظمة الطاقة والمياه والنقل وأنظمة الاتصالات والرعاية الصحية والمستشفيات والوظائف الأساسيّة اللازمة للحفاظ على سير الحياة في البلد بشكل طبيعي.

لم يكن لبنان بعيداً أو بمنأى عن هذه الأخطار التي لم تستثنِ أحداً منذ انتشارها الواسع بعد حوالي ثلاثة عقود من هيمنة شبكة الإنترنت، بل كانت المؤسّسات والإدارات الرسمية والشركات الخاصة والأفراد في الكثير من الأحيان هدفاً مباشراً لجرائم وهجمات سيبرانيّة أدّت في أغلب الحالات إلى خسائر هائلة على الصعيد

المادي وحتى البشري.

مصائب فوق مصائب

تمّ حذف الداتا واسترجعت بعد حين»، يروي رئيس مصلحة النقل البرّي في المديرية العامّة للنقل البرّي والبحري التابعة لوزارة الأشغال العامّة والنقل طوني عسّاف لـ«القوس» وقائع هجومين حدثا خلال الأشهر الفائتة، واستهدفا البيانات في المديريّة.

الهجوم الأوّل، في تشرين الأول 2022

«حضرت إلى مكان عملي وشغّلت جهاز الكمبيوتر فلم يعمل. بعد لحظات خرجت ورقة من آلة الفاكس عليها العبارة الآتية: نحن مجموعة هاكرز من الصّين، لقد تمّت سرقة الداتا الخاصّة بكم وحرمانكم من الولوج إليها على الأجهزة، ادفعوا لنا فدية لاسترجاعها!» يوضح عساف. دُفعت الفدية في المرّة الأولى للقراصنة (Hackers) لاسترجاع المعلومات. وأجرى التقنيون عملية النسخ الاحتياطي (Backup) على سيرفر – server مختلف، وبعد تلقّي رسالة القراصنة، تمّ التواصل مع مهندس المعلوماتية الخاصّ بالمديرية لأخذ الإجراءات والاحتياطات المناسبة، وبمساعدة شركة سايبر محليّة جرى تثبيت برنامج حماية عادي في المؤسّسة.

الهجوم الثاني، في آذار 2023

«بعد الهجوم الأوّل، طُلب منّا وضع برمجية حماية شاملة لكلّ تفاصيل المؤسّسة، لكنّ كلفته العالية لا تتناسب مع الإمكانات الماديّة المحدودة لدينا» يضيف عساف. إلى أن وقع الهجوم الثاني فلجأت المديرية إلى شركة خاصّة قامت بالإجراءات المناسبة. «لم نتواصل هذه المرّة مع الجهة المهاجمة، ولم نستجب لطلباتها. لجأنا إلى معهد تقني يتعاون مع شركة IT (تكنولوجيا المعلومات) خاصّة لمساعدتنا». استرجعت غالبية المعلومات. وعند التواصل مع فرع المعلومات ومكتب مكافحة الجرائم المعلوماتية (قوى الأمن الداخلي)، طُلب منّهم تقديم شكوى لدى النيابة العامّة، «لكنّنا لم نذهب لتقديم الشكوى لاعتقادنا بعدم جدوى الأمر، وظنًا منّا بأنّ الجهات الأمنيّة ستتحرّك فوراً لإجراء التحقيقات والتحريات وإعطاء الإرشادات بما أنّنا مؤسّسة حكومية تابعة للدولة!» يقول عسّاف. وذلك بطبيعة الحال يمسّ بمعطيات حسّاسة ما يسبّب خطراً على أمن المعلومات وقواعد البيانات الرسميّة. ونظراً إلى ضيق الوقت وضرورة المسارعة إلى تنفيذ إجراءات حمائية، لجؤوا إلى شركة خاصّة تعنى بالأمن السيبراني لمعالجة المشكلة.

حذّرتهم، (loss in data) كانت هناك خسائر في البيانات والمعلومات شركة أمن المعلومات التي استعانوا بها من ضعف برمجيات الحماية، إضافة إلى الإجراءات المتّبعة التي قد يصعب تطبيقها، وقالت إنّه «يمكن لطفل ذي خبرة قليلة أن يقوم بهجوم مماثل، وقد يكون ذلك بهدف التسلية!» مثل هجمات طلب الفدية (Ransomware Attack).

ويشير عسّاف إلى أن «في السابق، كنّا نعتمد في حالات مشابهة على قسم التنمية الإداريّة لكن أكثرية الموظّفين (لا سيّما تقنيّو وفنيّو الكمبيوتر) إمّا أحيلوا إلى التقاعد أو تركوا مراكزهم بحثاً عن فرص أفضل نظراً إلى تردّي الأوضاع، وبالتالي لم يعد هناك أحد ليقدم المساعدة اللازمة في تأمين الشبكات وحماية البيانات والمعلومات لدينا».
هذه الحادثة ليست الأولى وبالطبع لن تكون الأخيرة، فقد تعرّض العديد من الإدارات الرسمية اللبنانية في السنوات الماضية لهجمات إلكترونية (كاختراق مواقع حكومية مثل موقع وزارة التربية على الإنترنت، وضعف الحماية على منصّة Impact، الأمر الذي عرّض بيانات شريحة كبرى من اللبنانيين لخطر الاختراق. كذلك تعرّض بيانات وزارة الاتصالات لمحاولة اختراق وسرقة، وقرصنة معلومات وبيانات وبيعها في منتديات الإنترنت المظلم (Dark Web – تكمن الخطورة في العديد من الأحيان بحصول تسريب معلومات من داخل المؤسّسة من قبل أفراد نتيجة لعدم الانتباه أو الاكتراث لأدنى معايير الحيطة أو لأسباب أخرى.

في بلد يعاني من أزمات سياسية واقتصادية ومعيشيّة متتالية، ويفتقر إلى الحدّ الأدنى من الخدمات الأساسيّة وإلى الإمكانات المادّية اللازمة، قد لا يشكّل الأمن السيبراني أولوية لدى الجهات المعنيّة في الدولة نظراً إلى الإهمال وعدم الاكتراث، أو في أفضل الأحوال قد يترك الأمر على عاتق شركات السايبر الخاصّة والخبراء والكوادر من المتخصّصين في المجال الذين قد يؤمّنون الحلول، ولكن بتكاليف باهظة.

الفساد السيبراني

في الحالات التي تنجح فيها هذه الهجمات، يمكن أن تكون العواقب أضراراً مالية هائلة وحتّى خسائر في الأرواح البشرية (عندما تستهدف الهجمات القطاعات الصحيّة والطبّية، قد تنجم عن ذلك خسائر في الأرواح كما حصل حول العالم في فترة انتشار «كورونا»، بالإضافة إلى عمليات احتيال كبيع لقاحات مزيّفة عبر الإنترنت).
أضافة إلى تطوّر الصراعات والحروب التي أخذت طابعاً افتراضياً في

ملعب الفضاء السيبراني في السنوات الأخيرة، مع العديد من الحالات الموثّقة للهجمات الإلكترونية الخطيرة التي نفّذتها جماعات ومنظّمات ورعتها دول واستهدفت مرافق حكوميّة وبنى تحتية أساسيّة (كما يحصل بين دول عدّة في العالم: روسيّا وأوكرانيا، الصّين وأميركا، إيران والكيان الإسرائيلي..)
تستهدف هذه الهجمات أنظمة حيوية (شبكات الطاقة والكهرباء والاتصالات، وإمدادات المياه، وشبكات النقل، والجامعات، والمستشفيات، والمؤسّسات الماليّة والمصارف، وقواعد البيانات، وداتا الاتصالات، ووسائل إعلام، وصحافيين، وشخصيات سياسية..) وكلّ المجالات والقطاعات التي تحوّلت إلى رقمية، وباتت مرتبطة بالشبكة، بهدف تعطيل الخدمات الأساسية والتسبّب في أضرار واسعة النطاق.

بلد أعزل

لا تملك الدولة اللبنانيّة الحدّ الأدنى من الحلول والإمكانات والتقنيات التي يجب أن تواكب التحديات والمخاطر السيبرانية التي تجتاح العالم وتهدّد أمن مستخدمي شبكة الإنترنت. وفي الواقع، هذه الهجمات لن تتوقّف، بل ستكون أشدّ فتكاً وتعقيداً في المستقبل القريب وستستهدف مختلف القطاعات والمجالات. لذا فإنّ الحلّ يكمن في إجراءات الحماية والوقاية ووضع خطط عمل لا سيّما في الحالات التي ينجح فيها التهديد والهجوم في تحقيق أهدافه وذلك من أجل تقليل الخسائر.
ومن المهمّ تنفيذ استراتيجية أمن سيبراني شاملة والسعي لفهم ومعرفة أفضل السبل لتأمين الحماية الإلكترونية للأنظمة في المؤسّسات وفي القطاعات المختلفة، وأيضاً نشر التوعية والتثقيف على مستوى الأفراد.. إذ إن توعية الموظّفين والفرق التقنيّة والعاملين في القطاعات التي تتطلّب رقمنة ومكننة تعدّ أولويّة قصوى (من أكبر المخاطر التي تهدّد الأمن هي استغلال الأخطاء البشريّة والفرديّة لا سيّما في خروقات مثل هجمات الهندسة الاجتماعية).
إضافة إلى العمل على تخصيص ميزانيات كافية وزيادة التمويل وإيلاء الاهتمام لتأمين القطاعات الحيوية. ومن الضروري أيضاً في مواجهة هذا التحدي، اتخاذ خطوات استباقية لحماية البنية التحتية الرقمية من تهديدات الأمن السيبراني. وإدراك أهمية التعاون بين مختلف القطاعات بحيث يمكن للجامعات والمؤسّسات الأكاديميّة والشركات والخبراء أن يساعدوا في تمكين الكوادر والموظّفين في مؤسّسات الدولة، وتدريبهم على استخدام أفضل البرمجيّات والتقنيات

والإجراءات والأساليب التي يمكن أن تساهم في تحصين أمن الشبكات والمعلومات لمواجهة أي هجوم محتمل، نذكر منها:

– Software and Hardware Updates: تحديث التطبيقات والبرامج والمعدّات والأجهزة التقنية بشكل مستمرّ.
– Penetration Test: أي اختبار الاختراق وهو محاكاة لهجوم حقيقي مصرّح به يُجرى على الأنظمة والشبكات لتقييم أمانها، ويستخدم عادةً مختبرو الاختراق ذات الأدوات والتقنيات التي يستخدمها المهاجمون وذلك لإيجاد الثغرات ومكامن الضعف في الأنظمة والعمل على معالجتها وتأمين الحلول لها.
– Compromise Assessment: أي تقييم المخاطر السيبرانية والخروقات، وتحديد التهديدات الكامنة في شبكة المؤسّسة من خلال مؤشّرات الاختراق، ومن ثمّ التحقيق بالنتائج واتخاذ الإجراءات المناسبة.
تفعيل (NOC) ومركز عمليّات الشبكة (SOC) – مركز عمليّات الأمن: مراكز عمليات الأمن التي تقع على عاتقها مسؤولية مراقبة وحماية المؤسّسة من التهديدات السيبرانية، وأيضاً مراكز عمليّات الشبكة المسؤولة عن صيانة البنية التحتيّة للأنظمة والعمل على منع تداخلات الشبكة الناتجة عن الكوارث الطبيعية أو حالات انقطاع التيّار الكهربائي وانقطاع الإنترنت.

ولا بدّ أيضاً من الإشارة إلى ضرورة تفعيل عمل الأجهزة الأمنية والقضائية المعنيّة إلى الحد الأقصى نظراً إلى خطورة هجمات كهذه وحساسيّتها، والعمل على تعديلات قانونية تماهياً مع التطورات الحاصلة على مستوى العالم، ولا سيّما في ما يتعلّق بقوانين جرائم المعلوماتية ومكافحتها.

أبرز الهجمات التي تعرّضت لها مؤسّسات الدولة أخيراً، وأبرز نقاط الضعف:

تتعرض العديد من مؤسسات الدولة إلى خروقات سيبرانية من قبل جهات عدة قد تكون داخلية أو خارجية (قراصنة يعملون لانفسهم ومصلحتهم الشخصية، او لصالح جهات خارجية او معادية، او لشركات إعلانات تبغي الربح)

وزارة الداخلية

دانا وزارة الداخلية (**بيانات 3 ملايين مواطن**) مقرصنة وتباع في منتديات الشبكة المظلمة (الدارك ويب)

لمؤسسة كهرباء لبنان

سرقة وبيع **2000 حساب بريد إلكتروني** تابعين لمؤسسة كهرباء لبنان من قبل مقرصنة (مقابل دولار واحد!)

وزارة الإعلام

سرقة **أرشيف وسيرفرات** من مبنى وزارة الإعلام (سرقة معلومات Physical Security)

النافعة

سرقة **دانا** النافعة (هيئة إدارة السير والآليات والمركبات)، وتسريب **بيانات (اسماء وعناوين وارقام هواتف افراد)** من قبل موظفين في المؤسسة

أوجيرو

مشكلة **عدم صيانة وتحديث البنى التحتية** في هيئة أوجيرو التابعة لوزارة الاتصالات (تعريض الشبكات في لبنان لضعف في الحماية وخطر الاختراق)

وزارة المالية

موقع وزارة المالية (الذي يحتوي على بيانات لحسابات مالية وضرائب لمؤسسات وشركات ومصارف) **يفتقر إلى الحدّ الادنى من بروتوكولات الحماية (HTTPs)**

[المعلومات الواردة أعلاه مصدرها خبراء في الأمن السيبراني]

سلاح حربي غير تقليدي

في عصر الحروب الهجينة، وفي ظلّ الإمكانات التقنية الضخمة لدى العدو الإسرائيلي، وإلى جانب استخدامه برمجيات تجسّسية، لا بدّ من الإشارة إلى حتمية لجوئه في أي عدوان أو اعتداء على بلادنا إلى الهجمات السيبرانية (كهجمات الحرمان من الخدمة DDoS Attacks التي قد تعطّل خدمات الإنترنت)، والهجمات التي تستهدف البنية التحتيّة بهدف تعطيلها وتدميرها (مصادر طاقة، ومؤسّسات، ومصانع، وشبكات اتصالات، وقواعد بيانات..). إلى جانب التكتيكات التقليدية التي يلجأ إليها في العادة مثل هجوم القوات البريّة والضربات الجوّية. فمن خلال تعطيل أو منع الوصول إلى أيٍّ من هذه الموارد الحيوية، بإمكان العدو المهاجم التسبب بضرر أمني واقتصادي واجتماعي كبير في البلد.

ياسر الموسوي

المصدر: ملحق القوس بصحيفة الأخبار