بتاريخ: 13 أكتوبر 2021 العدد: 649 المصدر: اليوم السابع (2021/10/5)

انقطاع الـ 6 ساعات لمنصات فيس بوك.. ليلة مظلمة على السوشيال ميديا.. العالم في حيرة بدون فيس بوك و7 مليارات دولار خسائر زوكربيرج من صافي ثروته حتى الآن.. وواتس آب لم يعمل بشكل كامل

بدأت خدمات فيس بوك في العودة ببطء إلى الإنترنت بعد واحدة من أكبر حالات الانقطاع في الذاكرة الحديثة، ويبدو أن تطبيقات فيس بوك وانستجرام وماسنجر تعمل مرة أخرى، على الرغم من أن تحميل مواقع الويب أبطأ من المعتاد، وفي هذه الأثناء، يبدو أن موقع واتس آب الإلكتروني قد عاد في بعض المناطق، لكن التطبيق بشكل عام لا يزال يواجه مشكلات في الاتصال.

رابط الخبر

الرأي

ما شهده العالم من انقطاع لمنصات التواصل الاجتماعي والاستيلاء علي بيانات العملاء وتداولها أمر ليس بجديد وإنما تكرر مرارا، وإن كانت المرة الأخيرة الواردة بالخبر تعد الأطول زمنا والأوسع نطاقا. ورغم ضخامة التقديرات الأولية لبعض الخبراء حول الخسائر المالية الناتجة عن هذا الانقطاع والتي قد تصل لنحو 160 مليون دولار[1] إلا أن الأمر له أبعاد أخرى عديدة منها دور وأهمية الأمن السيبراني في تدارك مثل هذه القضايا، وهو محور هذا التعليق.

يعد الأمن السيبراني سلاح ذو حدين؛ فقد يلعب دورا داعما لتحقيق التنمية المستدامة، وقد يكون عائقا أمامها، لذا تظل قضايا حوكمة التكنولوجيا والمعايير الخاصة بالشفافية والخصوصية والحماية وغيرها محل اهتمام المجتمع الدولي بشكل مستمر. وقد أشار المنتدى الاقتصادي العالمي في تقرير التنافسية الصادر عام 2019 إلى أن وتيرة الابتكار في التكنولوجيات المرتبطة بالثورة الصناعية الرابعة تسير بطريقة تفوق كثيرا ما هو مبذول في مجال حوكمة هذه التكنولوجيات، لذا فهو تحدي جديد يواجه العالم المتقدم والنامي على السواء.

وقد وضع تقرير المخاطر العالمية الصادر عن المنتدى الاقتصادي العالمي لعام 2021 المخاطر السيبرانية ضمن أبرز المخاطر التي تهدد العالم خلال العشرة سنوات القادمة، كما من المتوقع أن يتضاعف حجم الخسائر التي تحملها العالم نتيجة الهجمات السيبرانية من نحو 5 تريليون دولار عام 2020 ليصل لنحو 10.5 تريليون دولار بحلول عام 2025.[2]

وتشير التقديرات إلى أن التكلفة الاقتصادية للهجمات السيبرانية للشركات التي تم دراستها في منطقة الشرق الأوسط وشمال إفريقيا عام 2021 تصل لنحو 6.9 مليون دولار للحادثة في المتوسط، أي أعلى من متوسط التكلفة العالمية البالغ نحو 4.2 مليون دولار للحادث، وأن الشركات الصغيرة والمتوسطة هي الأكثر تضررا .[3]

---

[1] https://twitter.com/netblocks/status/1445073059237466123?lang=en

[2] Cybercrime To Cost The World $10.5 Trillion Annually By 2025 (cybersecurityventures.com).

[3] IBM Security, “2021 Cost of a Data Breach Report”, available at: Enterprise Security | IBM

ومحليا، شهدت مصر العديد من المخاطر السيبرانية، وأحدثها إعلان بنك مصر عن سرقة 3 مليون جنيه من حسابات العملاء لديه من خلال اختراق بياناتهم في أغسطس 2021[4] غيرها العديد من المخاطر التي لا تفصح عنها الجهات خوفا من فقد ثقة عملائها فيها.

كل هذه الأحداث العالمية والمحلية تجدد وتؤكد على أهمية الأمن السيبراني باعتباره أحد محاور الأمن القومي خاصة بعد أن حفزت جائحة كورونا كافة الدول، ومنها مصر، على التحول الرقمي.

ومن حيث المبدأ، أدركت مصر أهمية تعزيز الأمن السيبراني؛ حيث تم تخصيص المادة رقم 31 من الدستور المصري الصادر عام 2014 للتأكيد على أن أمن الفضاء المعلوماتي (الأمن السيبراني) يشكل جزءا أساسيا من منظومة الاقتصاد والأمن القومي. وتلى ذلك العديد من الخطوات الجادة في هذا الاتجاه، ومنها إنشاء المجلس الأعلى للأمن السيبراني عام 2014[5]، وإطلاق الخطة الاستراتيجية الوطنية للأمن السيبراني 2017-2021، وتأسيس المركز الوطني للاستعداد لطوارئ الحاسبات والشبكات (EG-CERT). ولكن يبقي التساؤل الأهم عن مدى تفعيل هذه الجهود؟ خاصة وأنه وفقا لمؤشر الأمن السيبراني العالمي[6] الصادر عن الاتحاد الدولي لتنظيم الاتصالات لعام 2020 والصادر عام 2021 جاءت مصر في الترتيب 23 من بين 192 دولة وهو ترتيب متأخر إذا ما قورن بترتيب دول أخرى كالسعودية (2) والإمارات (5) والهند (10) مما يعكس وجود تحديات في الأبعاد المختلفة التي يغطيها المؤشر.

والتساؤل المطروح هو إلى أي مدى تعد الجهود التي تبنتها مصر كافية لتعزيز الأمن السيبراني ورفع درجة جاهزيتها بشريا وماديا وتكنولوجيا وتشريعيا ومؤسسيا للثورة التكنولوجية، وما تحمله من فرص وتهديدات ومخاطر. ويثير هذا التساؤل مجموعة من التساؤلات الفرعية:

---

[4] https://ar.scoopempire.com/%d8%b3%d8%b1%d9%82%d8%a9-%d8%ad%d9%88%d8%a7%d9%84%d9%8a-3-%d9%85%d9%84%d9%8a%d9%88%d9%86-%d8%ac%d9%86%d9%8a%d9%87-%d9%85%d9%86-%d8%b9%d9%85%d9%84%d8%a7%d8%a1-%d8%a8%d9%86%d9%83-%d9%85%d8%b5%d8%b1/

[5] قرار رئيس مجلس الوزراء رقم 2259 لسنة 2014.

[6] مؤشر مركب لمدى جاهزية الدول للأمن السيبراني وفقا لخمسة معايير هي: المعيار القانوني، المعيار التقني، المعيار التنظيمي، معيار بناء القدرات، معيار التعاون.

- إلى أي مدى تدرك الجهات المختلفة التحول الرقمي بمفهومه السليم، والذي يتجاوز الميكنة ويتضمن الأمن السيبراني كأحد ركائزه؟
- إلى أي مدى يتم ربط استراتيجية الأمن السيبراني ومجالات الاستثمار فيه بخطط الدولة للتنمية الاقتصادية والاجتماعية والاستثمارية؟
- هل يوجد تنسيق فعال بين الجهات المسئولة عن الامن السيبراني والجهات المسئولة عن التحول الرقمي؟
- إلى أي مدى يوجد دور حقيقي للقطاع الخاص في جهود الدولة للأمن السيبراني وفي الاستثمارات المحتملة في هذا المجال؟
- ما مدى كفاية وكفاءة خدمات المركز الوطني للاستعداد لطوارئ الحاسبات والشبكات ومدى استفادة مؤسسات القطاع الخاص والأهلي من خدماته؟
- ما معدل تنفيذ الأهداف التي وردت في الاستراتيجية الوطنية للأمن السيبراني 2017-2021 خاصة وأنها لم تسند مهام لجهات محددة ولم تتضمن مؤشرات أداء لمتابعتها ثم تقييمها؟
- هل إعداد الاستراتيجية الجديدة التي يتم إعدادها حاليا تلافى مشكلات الاستراتيجية السابقة؟
- إلى أي مدى يتم العمل على استكمال البنية التشريعية للأمن السيبراني سواء من خلال قوانين جديدة تخص إدارة البيانات، الهوية الرقمية أو من خلال تطوير تشريعات قائمة؟
- هل يتم رفع القدرات الحكومية في الموضوعات المتعلقة بالأمن السيبراني بالشكل المطلوب كما وكيفا؟ وهل يوجد حوافز لضمان الاحتفاظ بالكوادر بعد تأهيلها؟
- ما هي جهود الدولة في نشر ثقافة الأمن السيبراني للمجتمع ككل وللقطاع الخاص بشكل محدد، خاصة وأن هناك اتجاه من بعض الدول لتقديم حوافز ضريبية للقطاع الخاص لتشجيعه على الاهتمام بقضايا الأمن السيبراني؟

وأخيرا، ينبغي التأكيد على ضرورة اعتبار الأمن السيبراني شرط ضروري لنجاح التحول الرقمي، وبالتالي لا ينبغي أن يقتصر توجه الدولة فقط على تحصيل إيرادات من المتعاملين بشكل تجاري على مواقع التواصل الاجتماعي، فالقضية لها أبعاد أكثر خطورة وتستدعي جهودا أكبر لحوكمة ما يمكن منها.

جدير بالذكر:

قام المركز بالعديد من الجهود لدعم الجهد الحكومي للتحول الرقمي بالشكل السليم وذلك من خلال تقييم الجهود الحالية وتحديد السياسات المطلوبة في ضوء أفضل الممارسات، حيث:

- بادر المركز في يناير 2019 بالتعاون مع وزارتي الاتصالات وتكنولوجيا المعلومات ووزارة التخطيط والتنمية الاقتصادية بعقد سلسلة ورش عمل بعنوان *"أجندة بحثية تفصيلية لدعم الجهد الحكومي للتحول الرقمي للاقتصاد المصري؛" وركزت **الورشة الثالثة منها المنعقدة بتاريخ 27 فبراير 2019 على قضية توليد وحماية المعلومات.
- نظم المركز في ديسمبر 2019، بالتعاون مع KPMG Egypt، مؤتمرا مشتركا بعنوان ***"إدارة الأمن السيبراني ومخاطره: بالتركيز على حالة مصر" (cyber Risk Management Summit: A State of Cyber Security and Security, Regulations and Trends in Egypt).[7]
- أصدر المركز دراسة حول مفاهيم ****التحول الرقمي وحوكمة الأمن السيبراني في يونيو 2020

المصادر:

World economic forum (WEF). 2021. Global Risks Report. 16th Edition, WEF: Geneva.

[7] https://home.kpmg/eg/en/home/events/2019/12/cyber_security_summit_2019.html

*"أجندة بحثية تفصيلية لدعم الجهد الحكومي للتحول الرقمي للاقتصاد المصري؛"

**الورشة الثالثة

***"إدارة الأمن السيبراني ومخاطره: بالتركيز على حالة مصر"

****التحول الرقمي وحوكمة الأمن السيبراني

———. 2019. Global Competitiveness Report. WEF: Geneva.

خشبة، ماجد وآخرون. 2021. الأبعاد التنموية والاستراتيجية للأمن السيبراني ودوره في دعم الاقتصادات الرقمية والمشفرة: مسارات التجربة المصرية في ضوء التجارب العالمية. معهد التخطيط القومي، سلسلة قضايا التخطيط والتنمية 325. معهد التخطيط القومي: القاهرة.