المركز السوري لدراسات الأمن والدفاع

إصلاح الأمن السيبراني في سورية:

توحيد المنصات، التدريب، وخطط الاستجابة

لورنس شمالي - هادي أحمد

ورقة تحليلية

2026/03/15

المركز السوري لدراسات
الأمن والدفاع

مسداد مؤسسة بحثية مستقلة غير ربحية مقرّها سورية، تُعنى بإعداد الدراسات والتحليلات المتخصصة في قضايا الأمن والدفاع. وتسعى المؤسسة إلى الإسهام في تطوير هذا الحقل على المستويين الوطني والإقليمي، عبر إنتاج معرفة علمية رصينة تسهم في فهم التحديات الأمنية والدفاعية وطرح مقاربات عملية للتعامل معها.

تطمح المؤسسة إلى أن تكون مرجعًا موثوقًا لصنّاع القرار والباحثين، ومنصة فكرية فاعلة في صياغة رؤى استراتيجية تستند إلى البحث المنهجي والتحليل المعمّق، مع ربط الدراسات النظرية بالوقائع الميدانية والتحولات الجارية على الأرض.

كما تولي اهتمامًا خاصًا برصد التحولات الجيوسياسية وتحليل السياسات الدفاعية على المستويين الإقليمي والدولي، وتعمل على تقديم إنتاج معرفي يعزز الوعي العام ويدعم بناء قرار أمني ودفاعي رشيد ومسؤول.

للاطلاع على المزيد، يمكن زيارة الموقع الإلكتروني..

Misdad.org

تمهيد

منذ بداية عام 2026 تعرّضت عدة مواقع حكومية سورية لهجمات سيبرانية متكررة[1]، وتزامنت بعضها مع لحظات توتر سياسي-عسكري، بما يوحي بأنّ جزءًا منها استهدف الإحراج السياسي والإرباك المعنوي أكثر من استهداف البيانات والبنية المعلوماتية التحتية. وبرزت حادثة اختراق موقع وزارة الإعلام السورية في 12 كانون الثاني/يناير 2026 عبر العبث بالواجهة الرئيسة ورفع رموز وشعارات، من بينها علم "قوات سوريا الديمقراطية (قسد)" وعلم "كردستان العراق"[2]، قبل أن تُعلن الجهات المعنية معالجة الخلل وتأمين الخوادم[3]. ويعزّز تزامن الواقعة مع اشتباكات حلب آنذاك قراءة الاختراق كرسالة سياسية في سياق صراع مفتوح، حتى إن لم يتطور إلى سرقة بيانات أو تعطيل شامل للخدمات.

ولم تقتصر التحديات على مواقع الويب؛ إذ سُجّلت أيضًا هجمات طالت قنوات التواصل الرسمية، ولا سيما الحسابات الحكومية على منصة "X" والتي تم اختراق بعضها واستمر لعدة ساعات قبل أن تتم إعادتها للسيطرة الرقمية الحكومية، وهو ما أعاد النقاش حول مستوى التأمين المعتمد للهوية الرقمية الرسمية، وأظهر أن سطح الهجوم لا يبدأ من الخوادم فحسب، بل يمتد إلى إدارة الحسابات والصلاحيات والنسخ الاحتياطية وآليات الاستعادة[4].

لم تكن عمليات الهجوم السيبراني هذه هي الأولى من نوعها، حيث سبقتها العديد من عمليات الهجوم السيبراني لمواقع حكومية سورية، فقد رصد مركز أمن المعلومات الوطني في عام 2025 محاولات عدة لاختراق وقرصنة بيانات حساسة من مواقع حكومية، ونتيجة لهذه المحاولات سعت وزارة الاتصالات وتقنية المعلومات إلى إنشاء دليل لتطوير وتحديث الأنظمة الأمنية وحماية المواقع الإلكترونية[5].

تعالج هذه الورقة واقع الأمن السيبراني في سورية، بالتركيز على الاختراقات التي طالت مواقع وحسابات رسمية خلال الفترة الماضية، وما كشفته من هشاشة تراكمت بفعل تراجع الاستثمار في البنية الرقمية وضعف إجراءات الحماية. وتستهدف الورقة اقتراح حلول قابلة للتطبيق داخل

---

[1] **"اختراقات رقمية وتضليل في خضم أحداث حلب 270 .. ألف هجوم سيبراني على مواقع حكومية"**، شبكة شام، 2026/01/12، شوهد في 2026/02/11، في: https://2u.pw/ccUI6

[2] **"اخترق مواقع وزارة الإعلام السورية كأداة للتعبير عن التوتر"**، العرب، 2026/01/12، شوهد في 2026/01/11، في: https://2u.pw/SQ5drT

[3] **"هجوم إلكتروني يستهدف موقع وزارة الإعلام ويتسبب في تعطيله"**، اليوم السابع، 2026/01/12، شوهد في 2026/02/11، في https://2u.pw/pcBPKt :

[4] **"الاتصالات :إجراءات لحماية الحسابات الحكومية وتعزيز الأمن السيبراني في سوريا"**، سانا، 2026/03/03، شوهد في 2026/03/03، في: https://2u.pw/x0vAbx

[5] **"وزارة الاتصالات :تعاملنا مع محاولات سيبرانية لاختراق مواقع سورية"**، الإخبارية السورية، 2026/06/14، شوهد في 2026/02/21، في: https://2u.pw/RwyOY

المؤسسات الحكومية لتحسين "الانضباط التقني" ورفع الجاهزية وتعزيز الأمن السيبراني، بما يقلل كلفة الاختراق سياسيًّا وتشغيليًّا، ويَحد من أثره على استمرارية الخدمات العامة، وكذلك مكافحة المعلومات المضللة التي يمكن أن تنتج عن عمليات اختراق كهذه مستقبلًا.

قراءة تقنية مبسطة لطبيعة التهديدات

لفهم الاختراقات الأخيرة بدقة أكبر يُستحسن التمييز بين نمطين رئيسيْن من الهجمات التي تواجه مواقع الويب والبرمجيات. إذ يتصل النمط الأول بالاختراقات "التقليدية" المبنية على ثغرات معروفة ومعلنة، ويعتمد المهاجمون هنا على نسخ قديمة من أنظمة إدارة المحتوى أو المكونات البرمجية (Libraries/Plugins) التي لم تُحدَّث، وتستهدفها أدوات مؤتمتة تمسح الإنترنت بحثًا عن أهداف سهلة. ويقود هذا النمط إلى نتيجة واضحة مفادها أن جزءًا كبيرًا من الاختراقات يمكن الحد منه عبر: "الانضباط التقني"، وتحديث دوري، وضبط إعدادات الخوادم، وتقليل الامتيازات، ومراقبة السجلات، وإغلاق المنافذ غير الضرورية. وهذا ما ينص عليه "الدليل الاسترشادي لتصميم المواقع الحكومية" الصادر عن الهيئة الوطنية لخدمة تقانة المعلومات[6].

ويرتبط النمط الثاني بهجمات "اليوم صفر" (Zero-Day Vulnerability) التي تستغل ثغرة غير مكتشفة أو غير معلنة[7]. ويُعد هذا النمط أخطر وأقل شيوعًا، ويرتبط في كثير من الحالات بجهات رسمية كالدول أو أجهزتها الاستخباراتية، ما يجعل مواجهته تعتمد على المرونة التشغيلية أكثر من الاكتفاء بإجراءات الوقاية التقليدية. وتبرز هنا أهمية النسخ الاحتياطي المعزول، وخطط الاستجابة للحوادث، وتشفير البيانات الحساسة، ومتابعة التحديثات في مجال التشفير وفك التشفير والمعايير العالمية له، وبروتوكولات الاستعادة السريعة لضمان استمرارية العمل حتى في حال وقوع اختراق متقدم.

باختصار فإن الأمن الرقمي مهمّة مستمرة وتحتاج جهدًا كبيرًا للمتابعة والضبط، وهذا يعني أن المدافع عليه أن يفترض دومًا أنه عرضة لمحاولات الاختراق، وأنه عليه أن يتابع آخر التحديثات والتطورات في المجال الذي يعمل فيه والأدوات التي يعتمد عليها لتفادي النمط الأول من الاختراقات، وأن يضع خططًا احتياطية للتعامل مع النمط الثاني.

---

[6] **"الدليل الاسترشادي لتصميم المواقع الحكومية"**، الهيئة الوطنية لخدمات تقانة المعلومات، 2025/11/01، شوهد في 2026/03/03، في: https://2u.pw/0ljqgC

[7] **"ما المقصود بالاستغلال دون انتظار؟"**، IBM، شوهد في 2026/03/03، في: https://2u.pw/efxodq

عامل بشري لا يقل خطورة: الهندسة الاجتماعية ورفع الوعي الرقمي

تستند بعض الاختراقات إلى الهندسة الاجتماعية التي تتلاعب بسلوك الضحية (المسؤول عن إدارة المواقع أو الحسابات) لاختراق النظام من الباب الأضعف، وهو المستخدم. ويظهر هذا الأسلوب عبر رسائل تصيّد، أو روابط خادعة، أو حملات معلومات مضللة تدفع الموظف أو المستخدم إلى تسليم بياناته طواعية.

وتزداد خطورة هذا النمط في بيئات تتراجع فيها الثقافة الرقمية، أو تغيب فيها سياسات واضحة لإدارة كلمات المرور والتوثيق متعدد العوامل والصلاحيات، أو عندما لا توجد قنوات رسمية موثوقة تنفي الإشاعات وتغلق مسارات التضليل. ويعني ذلك أن الاستثمار في التوعية والتدريب ليس عملًا ثانويًّا، بل طبقة حماية أساسية تقلل احتمال الاختراق حتى عندما تكون الأنظمة محدثة[8].

الفوضى الرقمية الموروثة: الحاجة إلى إطار موحّد بدل الحلول الجزئية

تعاني البنية الرقمية الحكومية من تشتت تقني وإداري؛ إذ تعمل مواقع المؤسسات بمعايير متفاوتة وخوادم غير متجانسة وإجراءات صيانة غير موحدة، ما يجعل تأمينها عملية مكلفة ومتعبة ومرشحة للفشل عند غياب فريق مركزي مختص. ويفرض هذا الواقع الانتقال من حلول فردية متفرقة إلى إطار عمل موحّد (Unified Framework) يركز على توحيد المعايير قبل توسيع الخدمات.

يُعد توحيد البنية التحتية خطوةً ذات أثر مباشر على الكلفة والفعالية؛ إذ يسهل الصيانة والتحديث والتأمين حين تتقارب أنظمة التشغيل وخوادم الويب وإعداداتها، مع الإبقاء على استثناءات محدودة للمواقع التي تتطلب بنى خاصة. وتأتي بعد ذلك قيمة الاعتماد المدروس على البرمجيات مفتوحة المصدر، ليس بوصفه حلًّا سحريًّا، بل لأنه يخفف عبء التطوير من الصفر ويستفيد من مجتمعات تحديث نشطة، مع ضرورة ضبط الحوكمة والتحديثات والإضافات لتجنب تحويل "السهولة" إلى ثغرة.

وفي هذا السياق، يَشيع الاستشهاد بأن مواقع حكومية حساسة جدًا تستخدم أنظمة إدارة محتوى واسعة الانتشار؛ وتظهر واجهة "ووردبريس"(WordPress) الرسمية مثالًا عامًّا على وجود

[8] محمد مخلوف، **"أهم وسائل اختراق الإلكترونية ..ماذا تعرف عن الهندسة الاجتماعية؟"** قناة العربية، 2025/01/24، شوهد في 2026/02/12، في https://2u.pw/Tq1hh :

موقع البيت الأبيض ضمن "معرض ووردبريس"، بما يدعم فكرة أن معيار الأمان لا يرتبط بكون المنصة شهيرة أو مفتوحة المصدر بقدر ما يرتبط بحوكمة النشر والتحديث والهندسة الأمنية.

وتتكامل هذه المقاربة مع توحيد الهوية البصرية والوظيفية للمواقع الحكومية التي تقدم خدمات متشابهة؛ فبناء قوالب موحدة قابلة لإعادة الاستخدام لا يخفض التكلفة فقط، بل يرسخ أيضًا تجربة استخدام مألوفة للمواطن، ويقلل نقاط الضعف الناتجة عن اختلافات التطوير العشوائية بين مؤسسة وأخرى.

توصيات لتعزيز الأمن السيبراني

إن تعزيز الأمن السيبراني يبدأ بتحصين البنية التحتية التقنية، ويمكن تشبيه الخوادم (السيرفرات) بالأبنية التي تتضمن مداخل متعددة يجب تأمينها بدقة. ولتحقيق ذلك، لا بد من إغلاق المنافذ المفتوحة التي قد يستغلها المخترقون للعبور إلى النظام، وتأمينها بكلمات مرور قوية، مع توجيه مسؤولي الأنظمة للتفكير بعقلية المهاجمين لتوقع مسارات الاختراق المحتملة وسد الثغرات بشكل استباقي. إلى جانب ذلك، تبرز الحاجة الماسة لتوظيف أنظمة وجدران الحماية (Firewalls) بوصفها بوابات خارجية للتحكم الدقيق في تدفق البيانات، مما يسمح بمرور البيانات الموثوقة ويحجب العناوين والمواقع المشبوهة[9].

وعلى مستوى البرمجيات والمواقع المُستضافة، فإن الخطر الأكبر غالبًا ما ينبع من الأكواد البرمجية الضعيفة، وهي تشبه "الأثاث المتهالك" الذي يوضع داخل بناء متين فيجعله عرضةً للاختراق. ولمواجهة هذا التحدي، ينبغي فرض رقابة صارمة تمنع رفع أي موقع إلكتروني أو استضافته على السيرفرات الحكومية والعامة قبل خضوعه لتفتيش دقيق يثبت خلوه من الثغرات، ومنحه ما يمكن إطلاق عليه "ختم الكود النظيف" الذي يؤكد سلامة برمجياته ومطابقتها لمعايير الأمان القياسية[10].

من ناحية أخرى، لا تقتصر توصيات الأمن السيبراني على الجوانب التقنية البحتة، بل تمتد لتشمل العامل البشري الذي يُعد الحلقة الأضعف في سلسلة الحماية. ونظرًا لاعتماد الكثير من الهجمات على تقنيات "الهندسة الاجتماعية" وخداع المستخدمين للحصول على بياناتهم، ينبغي على الحكومة والمجتمعات الرقمية السورية نشر ثقافة الأمن الرقمي بين كافة فئات المجتمع بمختلف الفئات العمرية. ويتطلب هذا التثقيف توعية الأفراد بخطورة فتح الروابط المجهولة،

[9] **"أزمة الإنترنت والاتصالات :ما هو واقع ومستقبل القطاع في سوريا؟ مع د.سنان حتاحت"**، تنوين بودكاست، 2026/02/20، شوهد في 2026/03/05، في: https://bit.ly/4b7ccsf

[10] المرجع السابق.

وتدريبهم على الآليات السليمة لحماية حساباتهم الشخصية، وكيفية الاستجابة الفعالة والتصرف السليم في حال التعرض لأي اختراق رقمي[11].

أخيرًا، تكتمل منظومة الحماية السيبرانية من خلال إرساء إطار قانوني واستراتيجي شامل. فعلى الصعيد التشريعي، يبرز المطلب المُلح بتحديث المنظومة القانونية السورية لتواكب طبيعة الجرائم الإلكترونية وتتوازى مع جهود التثقيف، مع فرض عقوبات قاسية تتيح ملاحقة المخترِقين وردع كل من تسول له نفسه سرقة البيانات، أما على الصعيد الاستراتيجي الوطني، وللتعامل مع التهديدات المتقدمة التي تشنها الجيوش الإلكترونية الدولية سواء من إسرائيل أو غيرها، وهنا تبرز ضرورة تبني الدولة السورية لعقيدة دفاعية رقمية واضحة، وتأسيس جيش إلكتروني وطني يمتلك القدرة والكفاءة لصد الهجمات المعقدة من مختلف الجبهات، والقيام بهجمات ردعية مضادة عند الاقتضاء لحماية السيادة الرقمية للبلاد[12].

منطق "الهيئة الموحّدة" كحل عملي منخفض الكلفة

يقود ما سبق إلى خلاصة مفادها أن تعزيز حماية البيانات والمواقع الرسمية يتطلب إنشاء جهة موحدة تتولى وضع المعايير وإدارة البنية التحتية وتوفير بيئة رقمية آمنة وجاهزة للاستخدام من قبل الوزارات والهيئات الحكومية، وذلك يؤدي إلى إزاحة عبء الأمن والصيانة عن كاهل المؤسسات الفردية ويسمح لها بالتركيز على تقديم الخدمات ومن جهة أخرى يسمح لها بالتركيز على جانب الأمن السيبراني وحماية البنية المعلوماتية للبلاد ككل. ويتقاطع هذا الاتجاه مع ما يُنشر رسميًّا عن جهود تطوير البنية السيبرانية ورصد محاولات الاختراق عبر قنوات حكومية، الأمر الذي يشير إلى وجود نواة مؤسسية يمكن البناء عليها لتقليل "الفوضى الرقمية" وتحويلها إلى حوكمة ومعايير وإجراءات قابلة للقياس.

[11] المرجع السابق.
[12] المرجع السابق.

المركز السوري لدراسات
الأمن والدفاع