NTRA
National Telecom Regulatory Authority
الجهاز القومي لتنظيم الإتصالات

تهديدات سيبرانية محتملة

EG|CERT
المركز الوطني للإستعداد لطوارئ
الحاسبات والشبكات

وحدة تحليل البرمجيات الخبيثة والحماية التابعة للمركز الوطني للاستعداد لطوارئ الحاسبات والشبكات (EG-CERT) تحث القائمين على الدفاع عن الأمن السيبراني وتأمينه الاستعداد لأي هجمات خبيثة محتملة حيث قامت **الوكالة الأمريكية للأمن السيبراني وأمن البنية التحتية (CISA) والمركز الكندي للأمن السيبراني (CCCS) باصدار نشرة تحذيرية نصت على مجموعة من الإجراءات والتدابير التي يجب على كل مؤسسة اتخاذها لحماية أصولها وشبكتها من التهديدات الإلكترونية الخطيرة المحتملة**؛ حيث أعلن المركزان أن جميع المؤسسات مُعرضة للتهديدات السيبرانية.

يمكن للتهديدات السيبرانية المحتملة أن تقوم بتعطيل الخدمات الحيوية والتأثير على السلامة العامة. و في واقع الأمر، أثرت الحوادث السيبرانية طوال العام الماضي على العديد من المؤسسات غير الربحية والشركات والمنشآت الأخرى في عدة قطاعات. والجدير بالذكر أن العديد من الجهات والكيانات العامة والخاصة في أوكرانيا قد تعرضت الأسبوع الماضي لسلسلة من الهجمات والحوادث السيبرانية الخبيثة، مثل حوادث تشويه موقع الويب (web defacement)؛ وقد أفادت تقارير صادرة من منشآت ومؤسسات القطاع الخاص عن وقوع هجمات تدميرية استهدفت أنظمتها بواسطة برامج خبيثة شبه تدميرية والتي أدت إلى إلحاق أضرار جسيمة بعملياتها الحيوية. وذكر المركز الأوكراني الوطني للأمن السيبراني أن المهاجمين الذين نفذوا تلك الهجمات الأخيرة ربما يكونوا قد استغلوا ثغرة أمنية في نظام Laravel October CMS لإدارة المحتوى (CVE-2021-32648) .

وقد أبدى الخبراء قلقًا بالغًا من استخدام المهاجمين للبرامج الخبيثة التدميرية لإن العديد من البرامج المماثلة - مثل برامج NotPetya وبرنامج الفدية المدمر WannaCry – تم استخدامه ونشره فيما سبق وذلك لإحداث أضرار هائلة وشاملة في البنية التحتية الحيوية. تهدف نشرة CISA Insights التحذيرية إلى ضمان تعرف القائمين على المؤسسات والشركات على المخاطر السيبرانية الحرجة وأنهم على علم بها حتى يتسنى لهم اتخاذ إجراءات عاجلة وقريبة المدى يمكن من خلالها الحد من احتمالية حدوث أي اختراق سيبراني وتقليل آثاره في حالة حدوثه.

"معاً نحمى"

لتقليل احتمالية حدوث أي اختراق سيبراني ، يجب القيام بما يلي:

- التأكد من أن الوصول عن بُعد إلى شبكة المؤسسة يتطلب استخدام المصادقة متعددة العوامل (multi-factor authentication).
- التأكد من أن البرامج المستخدمة يتم تحديثها بشكلٍ دوري.
- ضمان قيام تعطيل كافة المنافذ (ports) والبروتوكولات التي لا تُعتبر ضرورية لإنجاز مهام العمل.
- التأكد من أن موظفي إدارة تكنولوجيا المعلومات قد قاموا بمراجعة وتنفيذ الضوابط السيبرانية اللازمة في حالة استخدام المؤسسة للخدمات السحابية.

للكشف السريع والمبكر عن أي هجوم سيبرانى محتمل قم باتخاذ الإجراءات التالية:

. التأكد من الكشف عن أي نشاط غير معتاد يتم على شبكة المؤسسة وتقييمه بشكلٍ سريع. قم بتفعيل "التسجيل" بهدف التحقيق بشكل أفضل في أي مشكلات أو أحداث أمنية.
- التأكد من أن شبكة المؤسسة محمية ومؤَمنة بالكامل بواسطة برامج مكافحة الفيروسات/البرامج الخبيثة ومن أن البصمات التعريفية في هذه الأدوات يتم تحديثها باستمرار.
- إذا كنت تتعامل مع احدى بالمؤسسات الأوكرانية، فيجب أن تتوخى الحذر وتقوم بمراقبة وفحص حركة المرور على شبكة المؤسسة وعزلها عن باقي الأجهزة ويجب أيضًا القيام بعمل مراجعة دقيقة لضوابط الوصول لهذه الحركة.

للتأكد من جاهزية المؤسسة وقدرتها على مواجهة أي هجوم سيبرانى قم بما يلي:

- اختيار نقاط الاتصال الرئيسية التي ستتعامل مع أي حادث أمني مشتبه به وتحديد المهام/ المسؤوليات ذات الصلة داخل المؤسسة.
- ضمان توفر وجاهزية المتخصصين والموظفين الرئيسيين؛ وتحديد وسائل توفير الدعم المؤقت والمفاجئ للاستجابة لحادث معين.
- التأكد من أن جميع المشاركين يدركون مهامهم التي يجب أن يقوموا بها أثناء وقوع هجوم سيبرانى.

لتعزيز قدرة المؤسسة على مواجهة أي هجوم سيبراني يجب أن يتم:

- القيام باختبار الإجراءات الخاصة بعمل نسخ احتياطية من الملفات والبيانات لضمان إمكانية استعادة البيانات الهامة بسرعة في حالة تعرض المؤسسة لهجمات برامج الفدية أو أي هجوم سيبراني؛ ويجب أيضًا التأكد من عزل نسخ البيانات الاحتياطية وعدم اتصالها بشبكة المؤسسة.
- في حالة استخدام أنظمة التحكم الصناعية أو تقنية تشغيلية يجب عمل اختبار للضوابط اليدوية حتى يتم التأكد من أن الوظائف الحيوية ستظل قابلة للتشغيل في حالة خروج شبكة المؤسسة من الخدمة أو إصابتها بهجوم سيبراني.

إن وحدة تحليل البرمجيات الخبيثة والحماية بالمركز الوطني للاستعداد لطوارئ الحاسبات والشبكات (EG-CERT) على أتم الاستعداد لمساعدة المؤسسات والجهات الحكومية المصرية في حمايتها من أي تهديدات سيبرانية ومعاونتها في تعزيز نظام الأمن السيبراني من خلال خبراءها المكلفين بذلك وبواسطة الخدمات التي تقدمها. وفي حالة تعرض أي مؤسسة لأي هجوم سيبراني، يمكننا تقديم المساعدات اللازمة لها واستخدام المعلومات الخاصة بالحادث ومؤشرات الاختراق (indicators of compromise) والبصمات التعريفية للبرمجيات الخبيثة لحماية المؤسسات الأخرى حتى لا تقع ضحية لمثل هذه الحوادث في المستقبل.