

هل يحمي موردو المكتبة بيانات المستفيدين؟ سبعة أسئلة للتقييم

أليكس كارو، كريس ماركمان



المخلص:

ينطلق هذا المقال من تدقيق مستقل لإدارة مخاطر الأمن السبراني أجراه المؤلفان لشبكة مكتبات عامة في مطلع 2015، ومن بحث سابق لهما في جامعة كلارك، ليؤكد أن على المكتبيين، بوصفهم المسؤولين عن خدمات المعلومات، أن يتحققوا من أن موردي المحتوى وتقنية المعلومات يأخذون الأمن السبراني بجدية. ويقترح المقال إطار تقييم بسيطاً سماه (LibSec)، يضم سبعة معايير موزونة النقاط: سياسة الإبلاغ عن اختراق البيانات، وتشفير البيانات، والاحتفاظ بها، وسهولة قراءة شروط الخدمة، وخصوصية المستفيدين إزاء أدوات التتبع، والاتصالات الآمنة، والمشاركة في شبكات الإعلانات التي تُمنح الوزن الأكبر. ويشرح كيفية منح النقاط وسلم التقديرات، وكيفية تكرار التقييم دورياً ومقارنة نتائج، ويعرض ورقتي عمل نموذجيتين لمورد نظام متكامل ولخدمة تواصل اجتماعي افتراضية. ويخلص إلى أن الإطار وسيلة مجانية لا تتطلب معرفة متخصصة لتتبع تقدم المكتبة نحو ممارسات أمنية أفضل.

الكلمات المفتاحية: الأمن السبراني، إدارة مخاطر تقنية المعلومات، موردو المكتبات، خصوصية المستفيدين، التدقيق الأمني

مقدمة:

نظم المكتبات الحديثة مؤسسات عامة فريدة من حيث البنية التحتية المادية لتقنية المعلومات فيها (قواعد البيانات والخوادم، ومختبرات الحاسوب، وشبكات الواي فاي العامة)، وبيان رسالتها (الحرية الفكرية، وخصوصية البيانات)، ومواثيق أخلاقياتها. وهذا المزيج من الأهداف، حين يُقارَن بقانون باتريوت الأمريكي (USA PATRIOT Act) لعام 2001 وبالمعلومات الأحدث المتعلقة بالمراقبة الحكومية الواسعة لحركة الإنترنت، ينشئ مجموعة فريدة من مخاطر الأمن السبراني للمكتبات التي تقطع هذه الوعود لمستفيديها. وفضلاً عن ذلك، فإن الاستخدام الواسع للمصادقة أحادية العامل (single-factor authentication) وتزايد خفض ميزانيات المكتبات بسبب حالات الركود الاقتصادي الأخيرة يهيئان ظروفًا مواتية للمجرمين السبرانيين.

وفي عام 2015، وفي إطار برنامج ماجستير العلوم في تقنية المعلومات بجامعة كلارك، اختبر كريس ماركماني (ماجستير في علوم المكتبات والمعلومات، (MSLIS)) وأليكس كارو (ماجستير في الإدارة العامة، (MPA)) نتائج بحثهما في مقرر سابق بجامعة كلارك يتعلق بإدارة مخاطر تقنية المعلومات، وذلك من خلال تدقيق أمني طوعي لمكتبة عامة، فأنشأ برنامجًا لإدارة مخاطر الأمن السيبراني (Cyber Security Risk Management, CSRM) يهدف إلى معالجة هذه القضايا. وقد عُرضت خلاصة لبعض نتائجنا في المؤتمر الربيعي السنوي لعام 2015 لمكتبيتي الخدمات الفنية في نيو إنجلاند (New England Technical Services Librarians) في صورة عرض خاطف (lightning talk)، لكن التفاصيل الكاملة لهذا التقرير تبقى سرية بموجب اتفاقنا مع المكتبة. ولم يكن برنامج إدارة مخاطر الأمن السيبراني الذي أنشئ شاملاً بأي حال، لكن البحث الأولي أشار إلى أن كثيرًا من نظم المكتبات ستستفيد من برنامج أكثر رسمية لإدارة مخاطر تقنية المعلومات.

الجزء 1 - إطار التقييم (LibSec):

إذا بدت هذه مهمة شاقة، فلا تقلق! لا داعي إلى «إعادة اختراع العجلة» فيما يتعلق بإدارة مخاطر الأمن السيبراني؛ فثمة أطر جاهزة كثيرة، ومن السهل مواءمتها مع احتياجات مؤسستك. وعادةً ما يُستعان بمدقق خارجي لإنجاز هذا العمل ويُرجى أن يضيف قدرًا من الموضوعية على نتائجه، غير أن مكتبات كثيرة قد تجد هذه الخطوة الإضافية باهظة التكلفة. ومن ثم رأينا الحاجة إلى إنشاء أطر لتقييم إدارة المخاطر تكون سهلة الفهم للجمهور وسهلة الاستخدام للمكتبيين. واقتداءً بعمل المكتبي إريك هيلمان (Eric Hellman)، الذي كشف في سلسلة من التدوينات عن سياسات الخصوصية لدى كبار موردي الدوريات أن كثيرًا منها لم يرق إلى التوقعات، قمنا بـ«هندسة عكسية» لمعايير التقدير التي وضعها، في صورة إطار التقييم التالي، ووزنا درجة كل فئة بحسب أثرها الإجمالي في الأمن السيبراني للمستفيدين. ونسميه (LibSec). ويرد في القسم التالي وصف مفصل لكل معيار، ولكيفية استخدام هذا الإطار.

ومن المهم ملاحظة أن قيمة النقاط في هذا النظام مرنة عن قصد، لأننا ندرك أنه لا توجد مكتبتان متماثلتان، بمعنى أن بعض المعايير نسبية تبعًا لفئة الناس الذين يستخدمون مكتبك. فعلى سبيل المثال، قد تقدّر مكتبة قانونية أكاديمية في مدينة كبرى مدى وضوح شروط الخدمة لدى مورد ما تقديرًا مختلفًا تمامًا عن مكتبة عامة ريفية. وفي هذا النمط من إدارة مخاطر الأمن السيبراني، من المهم ألا يُراعى الرأي المهني للمكتبيين فحسب، بل أيضًا الطريقة التي سيفسر بها المستفيدون المعلومات نفسها. وثمة كذلك طيف واسع من الموردين أو المنظمات الأخرى التي تتعامل معها المكتبة، والتي يمكن أن تكون جزءًا من هذه العملية الشاملة، وفي بعض الحالات يمكن استبعاد فئات بأكملها لأنها لا تنطبق. وبعبارة أخرى، قد تختلف النتائج من حالة إلى أخرى. ومن المهم أيضًا ملاحظة أنه في الجولة الأولى من عملية التقييم هذه بإطار (LibSec)، قد يستغرق العثور على هذه المعلومات بعض الوقت، ومن المفيد أن توثق كيفية تحديد مدى الامتثال في مجال معين ومصادر المعلومات التي استندت إليها، مع الاحتفاظ بسجل، حتى يمكن إنجاز التقييمات المستقبلية في مدة أقصر.

المعيار	وصف موجز	قيمة النقاط
1. سياسة الإبلاغ عن اختراق البيانات	هل توجد عملية رسمية للإبلاغ عن اختراقات البيانات إن وقعت وحين تقع؟	+/- 1 نقطة
2. تشفير البيانات	إذا كان المورد يخزن بيانات المستخدمين، فهل هي مشفرة؟	+/- 1 نقطة

المعيار	وصف موجز	قيمة النقاط
3. الاحتفاظ بالبيانات	هل يحذف المورد سجلات تاريخ بحث المستخدمين بصفة منتظمة؟	+/- 1 نقطة
4. «سهولة استخدام» شروط الخدمة	هل يستطيع المستخدم العادي قراءة سياسة شروط الاستخدام لدى المورد وفهمها فهمًا تامًا؟	+/- 1 نقطة
5. خصوصية المستخدمين	هل يستخدم المورد (Google Analytics) أو برمجيات تتبع أخرى لمراقبة المستخدمين؟	+/- 1 نقطة
6. الاتصالات الآمنة	هل يفرض موقع المورد الاتصالات الآمنة وحدها؟ باستخدام (HTTPS) أو بروتوكول أكثر أمانًا؟	+/- 1 نقطة
7. شبكات الإعلانات	هل يشارك موقع المورد في شبكات إعلانية؟	+/- 6 نقاط

سلم التقديرات:

(A)	أكبر من 11 نقطة أو يساويها
(B)	أكبر من 10 نقاط أو يساويها
(C)	أكبر من 9 نقاط أو يساويها
(D)	أكبر من 7 نقاط أو يساويها
(F)	أقل من 6 نقاط أو يساويها

1. سياسة الإبلاغ عن اختراق البيانات:

هذه لحظة لافئة للمكثبات في الولايات المتحدة الأمريكية، لأنه في حين اعتمدت بعض الولايات متطلبات لسياسات الإبلاغ عن اختراق البيانات، لا يوجد إلزام فدرالي. فعلى سبيل المثال: لنفترض للحظة أن مقدم الخدمة الذي تستخدمه مكتبك لبث المحتوى الصوتي تعرّض لاختراق أمني معروف، ولديه ما يدعو إلى الاعتقاد بأن معلومات العملاء (بما فيها سجل استعارات المستخدمين) قد تعرضت للاختراق على يد مجرم سيبراني. فإذا لم تكن لدى المورد سياسة للإبلاغ عن اختراق البيانات، فهو لم يلتزم بإبلاغ مستخدمي نظامه حين يقع حدث كهذا، ولا يمكنك اتخاذ قرار مستدير بشأن الأداء الإجمالي لممارساته الأمنية لأنه لم يعلن أنه سيفصح عن هذه المعلومات طوعًا. ويحصل الموردون في هذه الفئة على +1 نقطة إذا كانت لديهم سياسة للإبلاغ عن اختراق البيانات تفي بمعايير المكتبة، و0 نقطة إذا لم تتوافر سياسة للإبلاغ عن اختراق البيانات، و-1 نقطة إذا كانت سياسة الإبلاغ عن اختراق البيانات لا تفي بمعايير المكتبة.

2. تشفير البيانات:

الجانب المخيف في أمن تقنية المعلومات أننا نعلم أن لا جهة محصنة تمامًا من الاختراق؛ فحتى المنظمات الحكومية ذات الأسماء المختصرة بثلاثة أحرف والميزانيات الهائلة تتعرض لاختراقات أمنية. فالمسألة ليست ما إذا كانت أنظمتك ستتعرض للهجوم، بل متى وكيف. وتشفير البيانات، إذا أحسن تنفيذه، خطوة بسيطة جدًا نحو ضمان ألا تكون معلومات مستفيديك هدفًا سهلًا في حال وقوع اختراق أمني. وقد يحتج المرء بأن تشفير البيانات لا جدوى

منه إذا كانت بيانات المستخدمين مجهولة الهوية، لكن ما يجب أن نأخذه في الحسبان هو أن هذا النوع من المعلومات كثيرًا ما يستخدمه المجرمون السيبرانيون في صورة مجمعة للمساعدة على شن هجمات مستقبلية. وتشفير البيانات خطوة بسيطة جدًا، وإشارة إلى وجود شكل من أشكال الإشراف على الأمن السيبراني لدى موردك. وعلى غرار المعيار الأول، يحصل الموردون على +1 نقطة لتشفير البيانات، وصفر نقاط إذا كانت هذه المعلومات غير معروفة أو غير واضحة، و-1 إذا تمكنت من التأكد من أنهم لا يشقرون بيانات المستخدمين.

3. الاحتفاظ بالبيانات:

كثير من النظم المتكاملة للمكتبات يحذف سجل البحث أو بيانات المستخدمين آليًا، ولكن ماذا عن النظم التي تتفاعل معها؟ الغرض من هذه الفئة ألا تُبنى أي افتراضات: هل سألت عن سياسة الاحتفاظ بالبيانات لديهم؟ هل لديهم سياسة أصلًا؟ وما الإجابة المقبولة لمؤسستك؟ ويحصل الموردون على +1 إذا كانت سياسة الاحتفاظ مقبولة لدى المكتبة، وصفر نقاط إذا كانت هذه المعلومات غير معروفة، و-1 نقطة إذا عدت سياسة الاحتفاظ غير مقبولة.

4. «سهولة استخدام» شروط الخدمة:

نصوص «شروط الخدمة» (Terms of Service, TOS) يكتبها المحامون عادةً، وهي ليست باللغة الصعوبة في الفهم فحسب، بل مرهقة القراءة أيضًا بسبب طولها. ومن الآثار الجانبية المؤسفة لذلك أن مستخدمين كثيرين يتجاوزونها بنقرة دون قراءة التفاصيل الدقيقة. ومن المهم أن تشجع المكتبات المستخدمين على قراءة نصوص شروط الخدمة، لأن ذلك يمكّن الناس من اتخاذ قرارات مستنيرة بشأن كيفية استخدام معلوماتهم الشخصية ومتى يريدون ذلك. فقد لا يكتثرت بعضهم، وقد يكتثرت كثيرًا، وقد يكتثرت بعضهم أكثر بكثير لو فهموا تمامًا المعلومات التي يوافقون على تسليمها وكيف يمكن استخدامها. ويحصل الموردون على +1 إذا كانت شروط الخدمة لديهم سهلة القراءة، وصفر نقاط إذا تعدّ العثور على شروط الخدمة، و-1 نقطة إذا كانت شروط الخدمة صعبة القراءة.

5. خصوصية المستخدمين:

تتعلق هذه الفئة تحديدًا بـ«تتبع النقرات» (click-tracking)، أو بالأنظمة العاملة في الخلفية مثل (Google Analytics) التي تعمل على نحو غير مرئي في مواقع الويب أو موارد الويب لجمع معلومات إحصائية عن الصفحات التي تُزار، ومدة زيارتها، وكيف وُصل إليها. وتستخدم مواقع كثيرة هذه الأدوات، وجدواها داخل نظم المكتبات موضع نقاش مستمر في سعيها إلى الموازنة بين الحاجة إلى مقاييس موثوقة وخصوصية المستخدمين. والحقيقة البسيطة أن الخيار الأكثر أمانًا هو تعطيل هذه الأدوات تمامًا، أو تقييد استخدامها تقييدًا شديدًا (وربما يُنص على ذلك في سياسة الاحتفاظ بالبيانات لدى المورد، أو في شروط الاستخدام). ويحصل الموردون على +1 نقطة إذا كانوا يحترمون خصوصية التصفح، و0 نقطة إذا عدّ هذا التتبع في حدود المعقول (كأن لا تتضمن النتائج عنوان (IP) مثلاً)، و-1 نقطة إذا كان استخدامهم للتتبع غير مقبول.

6. الاتصالات الآمنة:

تناولت جميع الفئات حتى الآن البيانات «الساكنة» (at rest)، أي المعلومات المخزنة على الأقراص الصلبة أو الوسائط الأخرى. أما في هذه الفئة فنطلب منك تقييم البيانات «أثناء النقل» (in transit)، أي في طريقها إلى حواسيب أخرى (مملوكة للمكتبة أو للمستخدمين). ومن السهل إلى حد كبير أن يكتشف حتى المجرمون السيبرانيون

المبتدئون البيانات غير المشفرة التي تمر عبر الشبكة، وثمة أدوات برمجية مجانية تؤدي كل العمل في هذا الصدد. ومع أن الاتصالات الآمنة ليست الحل «النهائي» لأمن البيانات، لأن بروتوكولات مثل (HTTPS) يمكن فك تشفيرها على مستوى الجدار الناري، فإنها، كالفئة 2 تمامًا، خطوة بسيطة يمكن اتخاذها. ويحصل الموردون على +1 نقطة لفرض الاتصالات الآمنة على شبكاتهم، وصفر نقاط إذا كانت هذه المعلومات غير معروفة، و-1 نقطة إذا كانت اتصالاتهم غير مشفرة أو غير آمنة.

7. شبكات الإعلانات:

الجنب المخيف في مشاركة المورد في شبكات الإعلانات أو استخدامه لها أنك أصبحت مضطرًا إلى أن تأخذ في الحسبان لا البنية التحتية الأمنية لموردك الخارجي وعلاقتها ببرنامج إدارة مخاطر الأمن السيبراني في مكتبك فحسب، بل أيضًا البنية التحتية لدى المعلنين الذين يتعامل معهم. وضع في الحسبان أيضًا أن شبكات إعلانية كثيرة تعيد بيع معلوماتها لمعلنين آخرين، وهو تصرف لا سيطرة لك عليه لأنهم وقّعوا اتفاقيات مع موردك، لا معك أنت، المكتبة، مباشرة. ولهذا يفوق وزن هذا المعيار الأخير المعايير من 1 إلى 6: فالمشاركة في شبكات الإعلانات تجعل كل ما عداها بلا قيمة إذا كان موردك يفعل الأشياء الصحيحة ثم يسلم بيانات المستفيدين نفسها إلى شبكة إعلانية لا علاقة لها بالمكتبة ولا اتفاقيات محددة معها بشأن الاحتفاظ بالبيانات أو تشفيرها. وليس هذا فحسب، بل إن المجرمين السيبرانيين شتوا فعليًا في السنوات الأخيرة هجمات سيبرانية عبر شبكات إعلانية قائمة. ونشجعك على الاحتكام إلى أفضل تقديراتك في هذه الفئة، لأن شبكات الإعلانات ليست كلها متشابهة، لكنها في الوضع المثالي ليست أمرًا ينبغي أن تحتاج إلى النظر فيه أصلًا. ولهذا السبب يمكنك منح +6 نقاط لعدم استخدام شبكات الإعلانات، وصفر نقاط إذا كان الأمر غير واضح، وما يصل إلى -6 نقاط بحسب كيفية استخدام الإعلانات.

الجزء 2 - كيفية استخدام (LibSec):

يرجى أن تدرك أن ورقة العمل التي يتناولها هذا المقال ليست في حد ذاتها إلا إطارًا للتقييم، وينبغي أن تُعد جزءًا صغيرًا فقط من برنامج إدارة مخاطر الأمن السيبراني الشامل في مكتبك. فتثقيف المستخدمين وموظفي المكتبة بشأن الأمن السيبراني من خلال برامج مثل مشروع حرية المكتبات (Library Freedom Project) مكّون رئيس آخر، لكن أيًا من الحلين وحده لا يستطيع أن يحل مسألة حماية بيانات المستخدمين والمكتبة بأكملها.

والقوة الحقيقية لإطار تقييم مثل (LibSec) لا تكمن في ملء الاستمارات مرة واحدة ثم الاكتفاء بذلك، بل في ملئها، وتحديد المجالات غير الواضحة (ربما تتضمن الجولة الأولى درجات «صفر» كثيرة)، وطرح أسئلة على موردك لم تُطرح من قبل قط. وبعد شهر أو سنة، وبعد جمع مزيد من البيانات، كرر العملية نفسها بتدوين جميع الموردين الذين ترتبط بهم مكتبك بعلاقة، وإكمال هذه الاستمارات مرة أخرى، ومقارنة «بطاقة التقييم» هذه ببطاقة العام الماضي (أو العام الذي قبله).

الخاتمة:

حظيت إدارة مخاطر الأمن السيبراني في المكتبات، والمكتبات العامة على وجه الخصوص، باهتمام في الآونة الأخيرة من خلال مبادرات مثل مشروع حرية المكتبات وغيره من خدمات التواصل الموجهة إلى المستفيدين. وفي الوقت نفسه، يمكن لعمليات التدقيق الأمني الداخلية، سواء أُجريت داخل المؤسسة أو عبر متعاقدين أمنيين خارجيين، أن تضمن ألا تسرّب نظم المكتبات عن غير قصد معلومات تحدد الهوية الشخصية، لكنها مكلفة وتستغرق

وقتًا طويلًا حين ينجزها مدققون خارجيون. ونظام التقدير (LibSec)، كما وُصف في هذا المقال، وسيلة مجانية لتتبع تقدم مكتبك نحو ممارسات أفضل في الأمن السيبراني، من خلال تحليل دقيق لعلاقاتك مع الموردين والبيانات التي يوّلدها المستفيدون ويصل إليها هؤلاء الموردون أو يستهلكونها. ولا يتطلب أي معرفة متخصصة تتجاوز طرح مجموعة الأسئلة الصحيحة على مورديك، وتقييم خدماتهم في سياق مكتبك.

ورقة العمل النموذجية 1 - مورد نظام متكامل للمكتبات (ILS):

يحصل المورد في المثال التالي على التقدير «(B)» في هذا النظام. وللحصول على (A)، سيتعين عليه إما أن يعلن سياسته للإبلاغ عن اختراق البيانات، وإما أن يحسن شروط الخدمة لديه لتكون أيسر للمستخدم.

المعيار	قيمة النقاط	المسوّغ
سياسة الإبلاغ عن اختراق البيانات	0	غير متاحة / غير معروفة في الوقت الحالي
تشفير البيانات	1+	البيانات مشفرة
الاحتفاظ بالبيانات	1+	يُحذف سجل البحث بانتظام
«سهولة استخدام» شروط الخدمة	0	درجة محايدة. صعوبة القراءة نوعًا ما وطويلة جدًا، لكن العثور عليها سهل.
خصوصية المستفيدين	1+	لا يُستخدم التتبع
الاتصالات الآمنة	1+	(HTTPS) مقفل
شبكات الإعلانات	6+	لا يستخدم الموقع إعلانات
مجموع النقاط	10 (B)	

ورقة العمل النموذجية 2 - وسيلة تواصل اجتماعي «الموقع (X)»:

يحصل المثال الافتراضي التالي لخدمة تواصل اجتماعي على التقدير «(F)» وفق نظام التقدير هذا، ويذكر ذلك بأن على المكتبات أن تنظر في كيفية إسهام استخدامها لوسائل التواصل الاجتماعي في زيادة الأمن السيبراني للمستفيدين أو إنقاذه. وبوصف ذلك إجراءً تصحيحيًا، يمكن عدّ هذا فرصة لتثقيف عامة الجمهور بشأن التصفح الآمن على الشبكة.

المعيار	قيمة النقاط	المسوّغ
سياسة الإبلاغ عن اختراق البيانات	1+	السياسة معلنة.
تشفير البيانات	1+	البيانات مشفرة
الاحتفاظ بالبيانات	1-	سجل البحث مقفل دائمًا.
«سهولة استخدام» شروط الخدمة	0	درجة محايدة. صعوبة القراءة نوعًا ما وطويلة جدًا، لكن العثور عليها سهل.

المعيار	قيمة النقاط	المسوّغ
خصوصية المستخدمين	0	تتبع مشاهدات الصفحات في صورة مجمعة دون ربطها مباشرة بالحسابات، غير أن التطبيقات أو الخدمات الخارجية المرتبطة المستخدمة في الموقع قد تشكل مخاطر إضافية على الخصوصية.
الاتصالات الآمنة	1+	(HTTPS) مفقّل
شبكات الإعلانات	6-	كل حركة المرور مراقبة مراقبة مكثفة.
مجموع النقاط	4- (F)	

المراجع:

- للاطلاع على عرض عام متقن البحث لجهود خصوصية الإنترنت في المملكة المتحدة والولايات المتحدة في علاقتها بالمكتبات في «حقبة ما بعد سنودن»، انظر مقال إيان كلارك (Ian Clark) المنشور عام 2016 في Journal of Radical Librarianship: <https://journal.radical librarianship.org/index.php/journal/article/view/12>
- «16 of the top 20 Research Journals Let Ad Networks Spy on Their Readers» (ست عشرة من أكبر عشرين دورية بحثية تسمح لشبكات الإعلانات بالتجسس على قرائها) <http://go-to-hellman.blogspot.com/2015/03/16-of-top-20-research-journals-let-ad.html>
- للاطلاع على مقارنة مثيرة للاهتمام لهذه المشكلة، انظر مشروع «Terms of Service; Didn't Read» (شروط الخدمة؛ لم أقرأها) <https://tosdr.org>
- برنامج Wireshark مثال واحد فقط. وثمة حرفيًا آلاف الدروس التعليمية على الإنترنت التي تشرح كيفية استخدامه. وللإطلاع على عرض سريع، شاهد مقطع يوتيوب هذا ومدته 7 دقائق: «HakTip - How to Capture Packets with Wireshark - Getting Started» <https://www.youtube.com/watch?v=6X5TwwGXHP0>
- انظر <http://www.networkworld.com/article/2161439/network-security/ssl-decryption-may-be-needed-for-security-reasons-but-employees-are-likely-to-fre.html> وهذه سمة شائعة في معظم «الجدران النارية من الجيل التالي» https://en.wikipedia.org/wiki/Next-Generation_Firewall
- وهو أمر يتوقع أن يصبح إعداداه أسهل، بعد الإصدار التجريبي العام لمنصة شهادات «SSL» على <https://letsencrypt.org>
- يقدم موقع Yahoo.com مثالاً حديثاً واحداً فقط، إذ اختطف مهاجمون شبكته الإعلانية مدّة من الزمن وتمكنوا من نشر «برمجيات خبيثة» (malware) إلى آلاف المستخدمين: <http://thehill.com/policy/cybersecurity/250171-hackers-hijack-yahoos-ad-network-for-a-full-week>