

الشفافية وأمن المصدر المفتوح: كيف نقيس صحة المشروعات؟

آنا خيمينيث سانتاماريا



الملخص:

يناقش المقال علاقة الشفافية بأمن مشروعات المصدر المفتوح، انطلاقًا من انتشار مكوناتها في التطبيقات واعتماد المؤسسات عليها، ويبين أن إتاحة الشيفرة وحدها لا تكفي، بل يلزم تعاون الفرق والمجتمعات والإفصاح عن التهديدات والثغرات لدعم التقييم والثقة. ويعرض مقاييس لصحة المجتمع واستدامته، مثل تركيز المساهمات لدى أفراد أو مؤسسات محددة، وتحديد المطورين الأساسيين، وسرعة الاستجابة للمسائل، وشارات الممارسات الجيدة. ويربط ذلك بعمل مكاتب برامج المصدر المفتوح ومشروع (CHAOSS) وأدوات تحليل بيانات المجتمعات. ويؤكد أهمية الاستثمار في متابعة المنظومة وقياس نشاطها وتنوع مساهميتها. وتبقى هذه المقاييس مؤشرات مساعدة لتقدير المخاطر والاستدامة في سياق المقال، ولا تمثل ضمانًا لخلو البرمجيات من الثغرات أو بديلًا للفحص الأمني.

الكلمات المفتاحية: أمن المصدر المفتوح، الشفافية، صحة المجتمعات، (CHAOSS)، استدامة البرمجيات

يهدف الأمر التنفيذي الحديث لإدارة بايدن بشأن الأمن السيبراني إلى تحسين ضمانات الأمن واستخدام الممارسات الجيدة. وتساعد الشفافية وسلامة أداء المشروع على تعزيز الأمن في صناعة البرمجيات كلها، خصوصًا الآن.

أمن البرمجيات هو اليوم أمن المصدر المفتوح:

ينقل المقال أن 92% من التطبيقات الحديثة تتضمن مكونات مفتوحة المصدر؛ ولذلك يعني تحسين الأمن عمومًا تحسين أمن هذه المكونات. ويرى الأمر التنفيذي أن الثقة بالبنية الرقمية ينبغي أن تتناسب مع جدارتها بالثقة وشفافيتها.

والشفافية ركن في ضمان الأمن، لأنها تبني الاطمئنان إلى التقنية، وبدونها تتبدد الثقة. ومن وسائل تحسين الأمن تعزيز شفافية مشروعاتنا. وتتيح الشفافية معلومات تساعد المستخدم على تقييم سلامة أدائها بطريقتين على الأقل.

الأولى التعاون بين الفرق والمجتمعات، اللازم لمواكبة معايير الأمن والخصوصية والسلامة المتغيرة. فالأمن عملية معقدة تشمل فرقاً داخل المؤسسة ومؤسسات متعددة بسبب الطبيعة المفتوحة. والثانية الإفصاح العام، الذي يتيح إعداد تقارير أمنية ونشرها سريعاً لتحديد التهديدات والثغرات المحتملة.

كيف نقيس الشفافية؟

ينبغي أن يكون المصدر المفتوح جزءاً أصيلاً من المؤسسة الحديثة التي تريد شفافية عالية. لكن الشفافية تتجاوز إتاحة الشفرة والمنتجات والتصاميم والخدمات وواجهات البرمجة؛ إنها التزام بالوضوح الكامل.

وتطورت المنظومة إلى مشروعات ومؤسسات تربطها علاقات متنوعة ومعقدة. وتتيح مكاتب برامج المصدر المفتوح للشركات والمؤسسات العامة والحكومات متابعة حجم منظومتها وصحتها، في المشروعات التي تستخدمها أو تنشرها أو تسهم فيها.

ومن طرائق قياس الشفافية تقييم إجابات الأسئلة الآتية عن صحة المجتمع. كم شخصاً يلزم لاستدامة المشروع؟ يقيس «معامل الحافلة» عدد المساهمين الذين قد يفقدون المشروع قبل أن يتوقف. ويسميه الأصل بهذا الاسم لافتراض غيابهم المفاجئ في حادث، ويحسب أصغر عدد من الأشخاص الذين يقدمون 50% من المساهمات ويعرضه بصرياً.

ومن المطورون الأساسيون؟ يساعد «نموذج البصلة» على تحديد الأكثر التزاماً ومن يعتمد المشروع عليهم. وما المؤسسات المشاركة في التطوير؟ إلى جانب عدد الشركات التي يقدم موظفوها إبداعات أو بلاغات أو شفرة، يحدد «معامل الفيل» الحد الأدنى للشركات التي تنجز نصف العمل.

وهل توجد شهادات أمنية؟ يورد الأصل شارة الممارسات الجيدة لمبادرة البنية الأساسية مثلاً على اتباع المشروع معايير محددة. وما درجة نشاط المجتمع؟ توجد مقاييس عديدة، منها سرعة الاستجابة وحل المسائل مقارنة بعدد المسائل التي لا تلقى استجابة.

وتندرج معظم الأسئلة في مقاييس مشروع (CHAOSS) التابع لمؤسسة لينكس، الذي يطور مجموعة معيارية من المقاييس والبرمجيات لتحديد مؤشرات صحة المجتمعات المفتوحة. وتُسهّل أداة (GrimoireLab) تحليل هذه المقاييس وإعداد تقاريرها.

أفكار ختامية:

انتشر المصدر المفتوح عالمياً منذ زمن، والأمر التنفيذي سبب آخر للتعامل بجدية مع منظومته التي يعتمد عليها القطاع العام والخاص. لكن ابتكاره يتبع منهجية خاصة لا تطابق العمليات التجارية التقليدية. ويتطلب استخدامه الاستثمار في مكاتب البرامج وقياس الشفافية بالنظر إلى صحة المشروع ونشاطه لتحقيق المستوى المطلوب من ضمان الأمن.

المراجع:

- <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/>
- <https://www.igi-global.com/dictionary/quantitative-security-assurance/70165>

- <https://blog.tidelift.com/open-source-is-everywhere-survey-results-part-1>
- <https://www.redhat.com/en/events/webinar/automating-system-security-and-compliance-standard-operating-system?intcmp=70160000000h1s6AAA>
- <https://www.redhat.com/en/resources/container-security-openshift-cloud-devops-whitepaper?intcmp=70160000000h1s6AAA>
- <https://chaoss.community/metric-bus-factor/>
- https://chaoss.github.io/grimoirelab-sigils/common/onion_analysis/
- <https://chaoss.community/metric-elephant-factor/>
- <https://chaoss.community/metric-cii-best-practices-badge/>
- <https://chaoss.community/metrics/>
- <https://techcrunch.com/2019/01/12/how-open-source-software-took-over-the-world/>
- <https://todogroup.org/guides/create-program/>