materiał prasowy, 15.01.2024 r.

**Linux Polska stworzył innowacyjny system do analizy ryzyka oprogramowania open source**

**W jaki sposób może zwiększyć ochronę firm i instytucji przed cyberatakami w 2024 roku?**

**Z prognoz PMR wynika, że cyberbezpieczeństwo znajduje się na liście priorytetowych działań wśród największych firm w Polsce, a najnowsze prognozy zakładają, że w 2024 roku wartość rynku wzrośnie do 2,5 mld zł. Niestabilna sytuacja w naszym regionie, rosnąca liczba i skuteczność cyberataków czy konieczność dostosowania się do zmian dyktowanych, m.in. przez Dyrektywę NIS2 – to jedne z głównych powodów, dla których biznes decyduje się zwiększyć wydatki na bezpieczeństwo systemów IT. Według Barometru KPMG, co piąta firma odnotowała wzmożoną aktywność ataków w związku z wojną.[[1]](#footnote-1) Najczęściej zagrożone są agencje rządowe, firmy z sektora IT czy organizacje krytycznej infrastruktury, która jest kluczowa dla ciągłości funkcjonowania państwa. Dlatego też Linux Polska podjął się wyzwania stworzenia innowacyjnego systemu analizy ryzyka, który pozwoli na lepszą ocenę bezpieczeństwa oprogramowania i zwiększy stabilność jego wykorzystania w ekosystemie IT. W czym tkwi innowacja względem dostępnych na rynku rozwiązań i czy można już z niego korzystać?**

Z każdym rokiem rośnie popularność wykorzystania oprogramowania open source w biznesie, a tym samym bezpieczeństwo jego kodu – tworzonego nierzadko przez dziesiątki czy setki tysięcy programistów na całym świecie – staje się dla organizacji kluczowe. Według danych ponad 90 proc. firm w całej Europie wykorzystuje otwarte oprogramowanie.[[2]](#footnote-2) Złożoność tworzonych aplikacji coraz częściej jednak utrudnia dotarcie do informacji o aktualności i bezpieczeństwie wybranych komponentów. Co to oznacza w praktyce dla organizacji? Nieświadomość potencjalnych zagrożeń, które z roku na rok są coraz większe.

**W odpowiedzi na te wyzwania Linux Polska podjęła się realizacji projektu stworzenia autorskiego, innowacyjnego systemu analizy ryzyka oprogramowania open source, który dostarcza wnikliwą ocenę w zakresie bezpieczeństwa oraz stabilności otwartego oprogramowania, jakiej do tej pory nie dawały żadne dostępne na rynku rozwiązania.** Uwzględniając dużo szerszy zakres parametrów podlegających ocenie, jak choćby licencje czy umowy. Prace trwały ponad rok, projekt uzyskał dofinansowanie ze środków Europejskiego Funduszu Rozwoju Regionalnego

*– Nadrzędny cel, jaki nam przyświecał to przede wszystkim dostarczenie firmom rozwiązania, które pozwoli uzyskać wiarygodne i pełne informacje na temat poziomu bezpieczeństwa projektów, a także korzystać z bezpiecznych pakietów oprogramowania. Dzięki temu organizacje będą mogły obniżać koszty i ryzyko związane z jego wykorzystaniem, a także będą mogły skuteczniej zarządzać ryzykiem technologicznym. System do analizy ryzyka to wynikowa najlepszych kompetencji, doświadczenia i wiedzy ponad 30 specjalistów – od developerów, inżynierów systemów operacyjnych czy inżynierów środowiska skonteneryzowanych, inżynierów CI/CD, po specjalistów procesów wytwórczych oraz UX Designerów. Obecnie prace skupiają się wokół wdrożenia efektów naszych prac B+R poprzez produkcyjne uruchomienie portalu dystrybucji bezpiecznego oprogramowania open source. Wraz z nim klientom zostanie udostępniony cały portfel usług uzupełniających, od utrzymania projektów po gotowe pakiety warstwy systemowej i aplikacyjnej. Prace są prowadzone w ścisłej współpracy z rynkiem, wzmacniane wnikliwymi analizami i badaniami potrzeb* **– mówi Dariusz Świąder, CEO Linux Polska.**

**Jak działa najnowszy system?**

Przede wszystkim oprócz podstawowej oceny podatności, które oferuje większość dostępnych na rynku narzędzi, system do analizy ryzyka oprogramowania open source od Linux Polska uwzględnia dodatkowe, kluczowe aspekty ryzyka, jak np. analiza składu oprogramowania i specyficzne zagrożenia związane z jego produkcją, rozwojem i utrzymaniem. System analizuje poszczególne elementy, a także wzajemne zależności występujące między nimi, dając skumulowany wskaźnik informujący o ryzyku. A to daje zdecydowanie większą wiedzę organizacji i możliwość prewencji zanim ewentualne „słabości” zostaną wykorzystane w cyberataku. Co ważne, rozwiązanie to będzie badało zgodność oprogramowania z rekomendacjami NSC (Narodowe Standardy Cyberbezpieczeństwa). Wychodzi ono również naprzeciw dyrektywie NIS2 oraz zaleceniom w zakresie bezpieczeństwa łańcucha dostaw, wyspecyfikowanym przez europejską organizację cyberbezpieczeństwa ENISA.

*– Patrząc z perspektywy obecnej sytuacji geopolitycznej, w tym także trwającej wojny w cyberprzestrzeni – dostępne na rynku rozwiązania mogą nie być wystarczające. Dlaczego? Większość narzędzi koncentruje się na krótkoterminowych aspektach bezpieczeństwa i działaniach polegających na rozwiązywaniu na bieżąco znalezionych problemów. Tymczasem łańcuch logistyczny oprogramowania obejmuje wszystkie procesy i działania związane z wytwarzaniem i dostarczaniem tego oprogramowania, a w szczególności także procesy wszystkich użytych komponentów i bibliotek. Dlatego też Linux Polska poszedł o krok dalej i stworzony przez nas system pozwala na analizę poszczególnych elementów i występujących między nimi zależności, w tym zależności pomiędzy samym oprogramowaniem a komponentami. Dzięki temu uzyskujemy pogłębiony i bardziej szczegółowy, skumulowanych wskaźnik informujący nas o ewentualnym ryzyku. To coś, czego do tej pory nie było na rynku* **– komentuje Tomasz Dziedzic, CTO Linux Polska.**

Kluczowe dla bezpieczeństwa systemów IT opartych o otwarty kod źródłowy jest zarządzanie podatnościami (ang. vulnerability management). Mimo, że ten obszar nie jest nowym zagadnieniem, to wiele firm dopiero teraz zaczyna dostrzegać, że bazowe rozwiązania, jak np. okazjonalne skanowanie ewentualnych słabości systemu są niewystarczające. Z tego względu z roku na rok rosną inwestycje w bardziej zaawansowane rozwiązania a także outsourcing. **Według Barometru KPMG, organizacje w Polsce planują zwiększać inwestycje we wszystkich obszarach zabezpieczeń przed cyberzagrożeniami. Z kolei 8 na 10 firm korzysta z outsourcinsgu przynajmniej jednej funkcji cyberbezpieczeństwa.**[[3]](#footnote-3)

- *Dzisiaj minimalizowanie powierzchni ataku i ogólnego narażenia na ryzyko wymaga od firm ciągłości w działaniu, które pozwoli szybciej dostrzegać podatności i sprawniej je naprawiać. Proces zarządzania ryzykiem staje się kluczowy szczególnie dla największych firm, w zakresie bezpieczeństwa systemów teleinformatycznych i zarządzania bezpieczeństwem organizacji. A żeby móc skutecznie i sprawnie zarządzać tym procesem – niezbędne jest posiadanie narzędzi, które automatyzują i usprawniają wybrane czynności. Takim narzędziem jest właśnie stworzony przez nas system, dzięki któremu Klienci mają możliwość analizy ryzyka takich czynników, jak pochodzenie geopolityczne oprogramowania, w jakim państwie odbywa się jego produkcja, podatności czy scoring historyczny, licencja na jakim jest dane oprogramowanie i ryzyko z nią związane, a wszystko to jest skoncentrowane w jednym miejscu, na naszym portalu, co znacznie ułatwia cały proces* **– Magdalena Lasecka, Director Project Management Office, Linux Polska.**

**Rozwiązanie dla największych?**

System do analizy ryzyka oprogramowania open source sprawdzi się przede wszystkim wśród przedsiębiorstw, które utrzymują własną infrastrukturę informatyczną oraz podmioty, które pozyskują lub chciałyby pozyskiwać oprogramowanie z projektów o otwartym kodzie źródłowym, w tym głównie dla sektora finansowego, telekomunikacyjnego czy administracji publicznej.

- *W najbliższych latach największym wyzwaniem dla firm będzie zmiana myślenia o bezpieczeństwie oraz inwestycja w rozwiązania, które będą je zapewniać lub zwiększać, w szczególności w obszarze rozwiązań bazujących na open source. Obecnie wiele podmiotów jako główną blokadę przed zwiększeniem wydatków na cyberbezpieczeństwo wskazuje niewystarczający budżet (57 proc. w badaniu Barometr KPMG), czy trudności w zatrudnianiu i utrzymaniu wykwalifikowanych pracowników (47 proc.). Wśród badanych ponad połowa przyznała, że kwestia bezpieczeństwa nie jest stale monitorowana w ich organizacjach, a jednocześnie 1/3 odpowiadających odnotowała wzrost intensywności ataków cybernetycznych w ostatnim czasie. Sądzimy jednak, że z każdym rokiem ten odsetek będzie się zmieniał, a wydarzenia związane choćby z wprowadzeniem nowych unijnych regulacji w zakresie cyberbezpieczeństwa przyspieszą inwestycje w nowe technologie* **– dodaje Tomasz Dziedzic.**

1. Branżometr cyberbezpieczeństwa, KPMG, 2023 r. [↑](#footnote-ref-1)
2. World of Open Source: Europe Spotlight 2023 [↑](#footnote-ref-2)
3. Branżometr cyberbezpieczeństwa, KPMG, 2023 r. [↑](#footnote-ref-3)