**Raport Fortinet: prawie połowa firm doświadczyła naruszenia bezpieczeństwa swoich aplikacji**

****

**W celu zapewnienia kluczowej dla biznesu płynności operacyjnej, coraz więcej firm stara się zapewnić pracownikom, klientom i partnerom biznesowym dostęp do aplikacji z jakiegokolwiek urządzenia połączonego z internetem. Jednak coraz więcej problemów sprawia prawidłowe zabezpieczanie oprogramowania przed cyberatakami.**

Przedsiębiorstwa wprowadzają do użytku coraz więcej aplikacji oraz zwiększają tempo ich aktualizacji. Jak wynika z [„2021 Application Security Report”](https://global.fortinet.com/lp-en-aws-app-security-report) opublikowanego na podstawie globalnego badania zrealizowanego przez Fortinet w partnerstwie z Cybersecurity Insiders, coraz częściej krytyczne oprogramowanie, na którym polegają przedsiębiorstwa i użytkownicy, jest bezpośrednio narażone na kontakt z niezaufanymi sieciami oraz interakcje z publicznymi aplikacjami internetowymi. Dlatego firmy powinny zwracać coraz więcej uwagi na prawidłowe ich zabezpieczanie, a tym samym danych swoich klientów i użytkowników.

**Jakie są wyzwania w zabezpieczaniu aplikacji?**

W ciągu ostatniego roku, przy większej niż kiedykolwiek liczbie pracowników zdalnych, przedsiębiorstwa musiały polegać na oprogramowaniu, aby zapewnić ciągłość działania krytycznych procedur biznesowych. 48% respondentów korzystało z ponad 100 pojedynczych aplikacji działających w ich środowisku, a 26% *–* z ponad 500. Ten znaczący wzrost spotęgował istniejące problemy stojące przed zespołami IT odpowiedzialnymi za bezpieczeństwo.

* **Przedsiębiorstwa nie są pewne poziomu zabezpieczeń swoich aplikacji**. Oprogramowanie coraz częściej ma dostęp do wrażliwych firmowych danych, dlatego tak ważna jest prawidłowa ochrona poufnych informacji. Tylko 43% organizacji jest bardzo lub wyjątkowo pewnych bezpieczeństwa swoich aplikacji, przy czym głównym problemem dla 46% respondentów jest odpowiednie zabezpieczenie danych.
* **Naruszenia bezpieczeństwa aplikacji są powszechne, a użytkownicy nie zawsze są ich świadomi.** 43% firm w przeszłości doświadczyło naruszeń bezpieczeństwa swojego oprogramowania. Ponad jedna trzecia respondentów (35%) przyznała jednak, że nie wie, kiedy ostatni raz do niego doszło. Warto zauważyć, że znane środowiska aplikacji internetowych, takie jak Drupal, vBulletin i PHP, konsekwentnie pojawiają się w pierwszej dziesiątce celów ataków cyberprzestępców.
* **Tempo wprowadzania aktualizacji oprogramowania utrudnia jego zabezpieczanie.** Konsekwentne i częste testowanie podatności aplikacji na zagrożenia i naruszenia bezpieczeństwa ma kluczowe znaczenie. Tylko co piąty respondent deklaruje, że testuje oprogramowanie za każdym razem, gdy zmienia jego kod.
* **Przedsiębiorstwom brakuje personelu wykwalifikowanego w zakresie cyberbezpieczeństwa, także chmurowego.** Wielu ankietowanych uważa, że nie posiada obecnie w swoich zespołach zasobów, które pozwoliłyby im nadążyć za rozwijającymi się nieustannie cyberzagrożeniami. Według 46% respondentów brak wykwalifikowanego personelu znajduje się na szczycie listy barier, jakie napotykają firmy podczas zabezpieczania swoich aplikacji internetowych. Luka w umiejętnościach jest znanym i stałym problemem, który raczej nie zostanie rozwiązany w najbliższym czasie. Jednym ze sposobów, w jaki firmy mogą próbować sobie z nim radzić, jest inwestowanie w narzędzia i procesy, które pomogą zautomatyzować zadania, wcześniej wykonywane ręcznie, związane z zapewnieniem bezpieczeństwa aplikacji.

**Informacje o raporcie:**

„The CyberSecurity Insiders 2021 Application Security Report” został opracowany przez firmę Fortinet we współpracy z CyberSecurity Insiders. Bazuje na wynikach badania, w którym wzięło udział 344 ekspertów ds. cyberbezpieczeństwa z całego świata. Celem sondażu było zidentyfikowanie wyzwań, przed którymi stoją specjaliści odpowiedzialni za zabezpieczanie aplikacji.