

# Statystyki dotyczące bezpieczeństwa sieciowego, które warto znać

Jak bezpieczna jest Twoja firma jeśli chodzi o bezpieczeństwo aplikacji internetowych?

## \$4.2m

Średni koszt incydentu naruszenia

## 26%

Procent naruszeń, które występują przez aplikacje internetowe

## 94

Ataki na dzień

### 26% incydentów wynika z podatnych aplikacji internetowych

- **Oddziaływanie aplikacji internetowych:** Najnowsze badania Verizon ujawniają, że 26% wszystkich incydentów naruszenia dotyczy ataków na aplikacje internetowe, co plasuje się na drugim miejscu pod względem częstotliwości ataków.
- **Częstotliwość ataków:** Analiza 7 milionów witryn wykazuje średnio 94 ataki dziennie na pojedyncze strony.
- **Złośliwe boty:** Strony internetowe również spotykają się z istotną aktywnością botów, średnio 2600 wizyt botów na tydzień. Nie wszystkie są złośliwe, ale wiele z nich poszukuje luk w zabezpieczeniach, aby je wykorzystać.

### Systemy zarządzania treścią ułatwiają życie, ale także zwiększają ryzyko eksploatacji.

- **Podatność CMS:** Około 18% witryn WordPress ma co najmniej jedną podatność, która czeka na wykorzystanie.
- **Wtyczki CMS:** Instalacja wtyczek znacząco zwiększa ryzyko naruszenia. Dodanie pięciu wtyczek do witryny WordPress niemal podwaja ryzyko kompromitacji!
- **Średni koszt naruszenia danych:** Średni koszt naruszenia danych wynosi 4,24 miliona dolarów, co podkreśla finansowy wpływ związany z incydentami związanymi z bezpieczeństwem.

# Jak zmniejszyć ryzyko przy użyciu Probely

- **Zaawansowane Skanowanie Podatności:** Probely stosuje zaawansowane narzędzia skanujące podatności, aby proaktywnie identyfikować i rozwiązywać potencjalne słabości w aplikacjach internetowych, zmniejszając ryzyko eksploatacji.
- **Monitorowanie Ciągłe:** Poprzez ciągłe monitorowanie, Probely pomaga organizacjom pozostawać czujnym wobec ewoluujących zagrożeń, szybko wykrywając i reagując na wszelkie podejrzanе działania lub podatności.
- **Wszechstronne Testowanie Bezpieczeństwa API:** Probely przeprowadza dokładne testy interfejsów API, identyfikując podatności i zapewniając bezpieczeństwo wymiany danych między różnymi aplikacjami oprogramowania.
- **Automatyczne Wykrywanie Słabości API:** Wykorzystując zaawansowane możliwości skanowania, Probely automatycznie wykrywa i usuwa słabości w API, zapewniając proaktywną ochronę przed potencjalnymi naruszeniami i nieautoryzowanym dostępem.

*Zaawansowane narzędzia skanowania podatności Probely proaktywnie identyfikują i usuwają potencjalne słabości w aplikacjach internetowych, minimalizując ryzyko ich wykorzystania. Ciągłe monitorowanie zapewnia ciągłą czujność, szybko wykrywając i reagując na pojawiające się zagrożenia, co umożliwia organizacjom skuteczną obronę przed atakami internetowymi.*