

Statystyki dotyczące bezpieczeństwa sieciowego, które warto znać

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

\$4.2m

Średni koszt naruszenia

26%

wszystkich naruszeń zaczyna się od aplikacji internetowych

94

Ataków dziennie

26% incydentów jest wynikiem podatności w aplikacjach 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 wszystkich ataków
- **Częstotliwość ataków:** Analiza 7 milionów stron internetowych ujawnia średnio 94 ataki dziennie na poszczególne witryny
- **Złośliwe boty:** Strony internetowe również spotykają się z znaczącą aktywnością botów, średnio 2600 wizyt botów tygodniowo. Nie wszystkie są złośliwe, ale duża ich część szuka luk w zabezpieczeniach do wykorzystania

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, że incydenty bezpieczeństwa generują znaczące straty finansowe.

Jak zmniejszyć ryzyko przy użyciu Probely

- **Zaawansowane skanowanie podatności:** Probely stosuje zaawansowane narzędzia skanujące podatności, aby proaktywnie identyfikować i eliminować potencjalne słabe punkty w aplikacjach internetowych, zmniejszając ryzyko ich wykorzystania.
- **Ciągły monitoring:** Dzięki ciągłemu monitorowaniu Probely pomaga organizacjom zachować czujność wobec ewoluujących zagrożeń, szybko wykrywając i reagując na wszelkie podejrzanе działania lub luki w zabezpieczeniach.
- **Kompleksowe testy bezpieczeństwa API:** Probely przeprowadza dokładne testy API, identyfikując luki w zabezpieczeniach i zapewniając bezpieczeństwo wymiany danych między różnymi aplikacjami.
- **Automatyczne wykrywanie słabych punktów API:** Probely wykorzystuje zaawansowane możliwości skanowania, aby automatycznie wykrywać i eliminować słabe punkty interfejsów API i zapewniać proaktywną ochronę przed 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, umożliwiając organizacjom skuteczną obronę przed atakami internetowymi.