RAZEM O CYBER

JAK MOŻEMY POMÓC PRZY WDROŻENIU NIS2

3 kwietnia 2026 r. wchodzą w życie nowe regulacje z zakresu cyberbezpieczeństwa, które implementują w Polsce dyrektywę NIS2.

Nowe cyberwymogi dotyczą aż 18 sektorów gospodarki, w tym m.in.: energii, transportu, bankowości i rynków finansowych, ochrony zdrowia, wody pitnej, ścieków, infrastruktury cyfrowej, usług cyfrowych, usług ICT, usług pocztowych, gospodarki odpadami, żywności, chemikaliów oraz produkcji (w szczególności wyrobów medycznych, urządzeń elektronicznych i pojazdów).

HARMONOGRAM DZIAŁAŃ

Do 3 października 2026 r.
Samoidentyfikacja i rejestracja jako podmiot kluczowy lub ważny

Do 3 kwietnia 2027 r.
Wdrożenie systemu zarządzania bezpieczeństwem informacji oraz przeprowadzenie szkoleń w organizacji

Do 3 kwietnia 2028 r.
Pierwszy audyt cyberbezpieczeństwa dla podmiotów kluczowych

POMOŻEMY CI WDROŻYĆ NOWE CYBERWYMOGI W ORGANIZACJI

- Samoidentyfikacja – sprawdzimy, czy jesteś podmiotem kluczowym lub ważnym oraz czy podlegasz nowym obowiązkom w Polsce.
- Rejestracja – wesprzemy Cię w procesie rejestracji jako podmiot kluczowy lub ważny.
- System bezpieczeństwa informacji – pomożemy we wdrożeniu systemu zarządzania bezpieczeństwem informacji w organizacji (polityki, procedury, analizy, procesy).
- Szkolenia – zapewnimy szkolenia z cyberbezpieczeństwa dla zarządu i pracowników oraz zaprojektujemy instrukcje dotyczące cyberhigieny.
- Relacje z dostawcami – przygotujemy umowy z dostawcami oprogramowania i sprzętu ICT, wesprzemy Cię przy negocjacjach takich umów w zakresie cyberbezpieczeństwa oraz zaprojektujemy proces weryfikacji dostawców.

BRAK WDROŻENIA NIS2 W ORGANIZACJI TO RYZYKO M.IN.:

- kar finansowych – kary pieniężne do 10 mln euro lub 2% rocznych przychodów (podmioty kluczowe) oraz do 7 mln euro lub 1,4% rocznych przychodów (podmioty ważne), przy czym zastosowanie ma kwota wyższa,
- osobistej odpowiedzialności zarządu – kary pieniężne dla członków zarządu do 300% wynagrodzenia oraz możliwość nałożenia zakazu pełnienia funkcji zarządczych do czasu usunięcia uchybień lub zaprzestania naruszeń (w podmiotach kluczowych),
- utraty reputacji – publiczne ujawnienie incydentu lub obowiązek powiadomienia klientów o incydencie,
- wysokich kosztów operacyjnych – koszty niedostępności systemów lub ich odtworzenia po incydencie często przewyższają koszty wdrożenia systemu zarządzania bezpieczeństwem informacji.

MASZ PYTANIA LUB NIE WIESZ OD CZEGO ZACZĄĆ WS. NIS2, SKONTAKTUJ SIĘ Z NAMI!

Jakub Kubalski
Partner
jakub.kubalski@ssw.solutions

Agnieszka Witaszek
Partner
agnieszka.witaszek@ssw.solutions