Oświadczenie TP-Link – Dyrektywa EU NIS2

Wrzesień 2025

TP-Link Systems Inc. potwierdza swoje zaangażowanie w cyberbezpieczeństwo i przestrzeganie przepisów, poprzez implementację zarządzania zgodnego ze standardami branżowymi, zarządzania ryzykiem i kontroli technicznych. W ramach tego zobowiązania, TP-Link otrzymał certyfikację w ramach normy **ISO/IEC 27001:2022 (**ISO/IEC 27001:2022**)**, rozpoznawalnego standardu na całym świecie dla Information Security Management Systems (ISMS), a także przyjął **Secure Product Development Lifecycle (SPDL)**

1. Certyfikacja ISO/IEC 27001:2022

ISMS TP-Link zostało certyfikowane zgodnie z normą ISO/IEC 27001:2022, która wymaga:

- Polityk dotyczących analizy ryzyka i bezpieczeństwa systemów informatycznych
- Zarządzania incydentami i podatnościami
- Kontroli nad bezpieczeństwem łańcucha dostaw
- Bezpiecznego cyklu rozwoju produktu
- Ciągłego monitorowania i poprawy mechanizmów

Na podstawie oficjalnych wytycznych ENISA (NIS2 Technical Implementation Guidance | ENISA), ta certyfikacja przedstawia zgodność TP-Link ze **środkami bezpieczeństwa** wyszczególnionymi w **Artykule 21 Dyrektywy NIS2.**

2. Odniesienia do Artykułu 21 Dyrektywy NIS2

Określona funkcja	**Klauzula Artykułu 21 NIS2**
Izolacja sieci oparta na VLAN	(g) podstawowe praktyki cyberhigieny i szkolenia w zakresie cyberbezpieczeństwa (i) bezpieczeństwo zasobów ludzkich, polityki kontroli dostępu i zarządzanie aktywami
Separacja sieci dla gości	(g) podstawowe praktyki cyberhigieny i szkolenia w zakresie cyberbezpieczeństwa (i) bezpieczeństwo zasobów ludzkich, polityki kontroli dostępu i zarządzanie aktywami
Kontrola dostępu do Kontrolera	(g) podstawowe praktyki cyberhigieny i szkolenia w zakresie cyberbezpieczeństwa (i) bezpieczeństwo zasobów ludzkich, polityki kontroli dostępu i zarządzanie aktywami
Uwierzytelnianie dwuetapowe i SAML SSO	(j) korzystanie z wieloetapowego uwierzytelniania lub rozwiązań ciągłego uwierzytelniania, zabezpieczona komunikacja głosowa, wideo i tekstowa, a także zabezpieczone systemy komunikacji alarmowej w obrębie jednostki, gdzie ma to zastosowanie
RBAC z obsługą własnych roli	(g) podstawowe praktyki cyberhigieny i szkolenia w zakresie cyberbezpieczeństwa (i) bezpieczeństwo zasobów ludzkich, polityki kontroli dostępu i zarządzanie aktywami
Reguły dostępu IP	(g) podstawowe praktyki cyberhigieny i szkolenia w zakresie cyberbezpieczeństwa (i) bezpieczeństwo zasobów ludzkich, polityki kontroli dostępu i zarządzanie aktywami
Kontrola dostępu oparta na czasie	(g) podstawowe praktyki cyberhigieny i szkolenia w zakresie cyberbezpieczeństwa (i) bezpieczeństwo zasobów ludzkich, polityki kontroli dostępu i zarządzanie aktywami

Kontrola dostępu klientów	(g) podstawowe praktyki cyberhigieny i szkolenia w zakresie cyberbezpieczeństwa (i) bezpieczeństwo zasobów ludzkich, polityki kontroli dostępu i zarządzanie aktywami
Integracja LDAP	(g) podstawowe praktyki cyberhigieny i szkolenia w zakresie cyberbezpieczeństwa (i) bezpieczeństwo zasobów ludzkich, polityki kontroli dostępu i zarządzanie aktywami
Zaawansowane zabezpieczenie WPA3	Polityki i procedury odnoszące się do kryptografii i tam gdzie ma to zastosowanie, do szyfrowania
Integracja RADIUS	(g) podstawowe praktyki cyberhigieny i szkolenia w zakresie cyberbezpieczeństwa (i) bezpieczeństwo zasobów ludzkich, polityki kontroli dostępu i zarządzanie aktywami
Filtrowanie adresów MAC	(g) podstawowe praktyki cyberhigieny i szkolenia w zakresie cyberbezpieczeństwa (i) bezpieczeństwo zasobów ludzkich, polityki kontroli dostępu i zarządzanie aktywami
Wykrywanie i zapobieganie włamaniom (IDS/IPS)	(a) polityki dotyczące analizy ryzyka i bezpieczeństwa systemów informatycznych (b) zajmowanie się incydentami
Ochrona przed DDoS	(a) polityki dotyczące analizy ryzyka i bezpieczeństwa systemów informatycznych (b) zajmowanie się incydentami
Reguły i polityki Firewall	(a) polityki dotyczące analizy ryzyka i bezpieczeństwa systemów informatycznych (b) zajmowanie się incydentami
Łączność VPN	(a) polityki dotyczące analizy ryzyka i bezpieczeństwa systemów informatycznych (b) zajmowanie się incydentami
Analiza ruchu sieciowego w czasie rzeczywistym	(a) polityki dotyczące analizy ryzyka i bezpieczeństwa systemów informatycznych (b) zajmowanie się incydentami
Monitorowanie łączności urządzenia	(a) polityki dotyczące analizy ryzyka i bezpieczeństwa systemów informatycznych (b) zajmowanie się incydentami
Śledzenie wykorzystania przepustowości	(a) polityki dotyczące analizy ryzyka i bezpieczeństwa systemów informatycznych (b) zajmowanie się incydentami
Rejestrowanie zdarzeń i Dziennik audytu	(a) polityki dotyczące analizy ryzyka i bezpieczeństwa systemów informatycznych (b) zajmowanie się incydentami (c) ciągłość działania, taka jak zarządzanie kopią zapasową, odzyskiwanie po awarii i zarządzanie kryzysowe