Wdrożenie środków cyberbezpieczeństwa w celu spełnienia wymogów NIS2

NIS2, czyli **Dyrektywa Unii Europejskiej 2022/2555**, ma na celu podniesienie ogólnego poziomu cyberbezpieczeństwa w UE oraz zapewnienie odporności sieci i systemów informatycznych podmiotów krytycznych działających w regionie. NIS2 to zasadniczo zestaw wymogów w zakresie cyberbezpieczeństwa dla organizacji z wielu branż o kluczowym znaczeniu dla gospodarki UE. Dyrektywa wymaga od tych organizacji wdrożenia określonych środków cyberbezpieczeństwa w celu zabezpieczenia ich sieci i systemów informatycznych.

NIS2 ma zastosowanie do następujących podmiotów działających w Unii Europejskiej:

Istotne podmioty (Aneks I do NIS2)

Ważne podmioty (Aneks II do NIS2)

Informacje o Ekran System

Ekran System to platforma do zarządzania ryzykiem wewnętrznym w pełnym cyklu, zaprojektowana w celu powstrzymywania, wykrywania i zapobiegania zagrożeniom wewnętrznym. Wyposażony w bogaty zestaw narzędzi, Ekran System może pomóc organizacji zwiększyć odporność cybernetyczną i wdrożyć większość wymagań NIS2 za pomocą jednego rozwiązania. Kluczowe funkcje Ekran System obejmują monitorowanie aktywności użytkowników, zarządzanie dostępem i reagowanie na incydenty.

Dostosowanie wymogów NIS2 do odpowiednich środków

Dyrektywa NIS2 nie zawiera żadnych konkretnych wyjaśnień dotyczących przedstawionych w niej środków, ale raczej oferuje ogólne cele w zakresie cyberbezpieczeństwa, których organizacje powinny przestrzegać. Z tego powodu przygotowaliśmy zestawienie prezentujące kluczowe środki, które można wdrożyć w celu spełnienia wymagań NIS2 za pomocą Ekran System, inicjatyw organizacyjnych i innych rozwiązań.

Wymaganie NIS2	Działania do wdrożenia					
Analiza ryzyka i bezpieczeństwa systemów informatycznych	Wykorzystaj monitorowanie aktywności użytkowników, aby zwiększyć widoczność infrastruktury IT i wykrywać zagrożenia wewnętrzne, luki w zabezpieczeniach i inne zagrożenia cyberbezpieczeństwa.	Szczegółowo zarządzaj dostępem użytkowników i monitoruj użytkowników uprzywilejowanych, aby zapobiec ryzyku nieautoryzowanych działań.	Opracuj polityki i procedury identyfikacji, oceny i priorytetyzacji zagrożeń cyberbezpieczeństwa.	Ustanów zasady bezpieczeństwa systemów informatycznych.	Wdróż system zarządzania bezpieczeństwem informacji (ISMS) opartego na normie ISO 27001.	Przeprowadź inwentaryzację wrażliwych zasobów i oprogramowania.
Obsługa i raportowanie incydentów	Umożliw wykrywanie złośliwej aktywności użytkowników i innych zagrożeń cyberbezpieczeństwa w czasie rzeczywistym.	Wdróż i zautomatyzuj szybkie reakcje na zagrożenia bezpieczeństwa.	Zapewnij badania incydentów z eksportem nagranych sesji do celów kryminalistycznych.	Opracuj plan roagowania na incydenty (IRP) określającego kroki, które należy podjąć w przypadku różnego rodzaju incydentów bezpieczeństwa.	Szybko zgłaszaj incydenty cyberbezpieczeństwa odpowiednim organom regulacyjnym i władzom, zgodnie z art. 23 dyrektywy NIS2.	Dokumentuj swoje procedury zgłaszania incydentów.
Ciągłość działania, taka jak zarządzanie kopiami zapasowymi i odzyskiwanie danych po awarii oraz zarządzanie kryzysowe	Szybko wykrywaj zdarzenia związanye z bezpieczeństwem, które mogą potencjalnie prowadzić do kryzysu.	Wykorzystaj nagrań sesji użytkowników i dzienników aktywności w celu oceny wpływu na systemy i dane oraz opracowania planów i procedur odzyskiwania danych.	Zmniejsz ryzyko nieautoryzowanych działań, które mogą zakłócić działalność biznesową, poprzez uzyskanie uprawnień dostępu w infrastrukturze IT.	Ułatwij komunikację poprzez dostarczanie dokładnych i szczegółowych informacji o kryzysie i jego skutkach.	Ustanów plan ciągłości działania (BCP), który obejmuje przepisy dotyczące zarządzania kopiami zapasowymi, odzyskiwania danych po awarii i zarządzania kryzysowego.	Wdróż regularne procedury tworzenia kopii zapasowych krytycznych danych i systemów.
Bezpieczeństwo łańcucha dostaw, w tym aspekty związane z bezpieczeństwem dotyczące relacji między każdym podmiotem a jego bezpośrednimi dostawcami lub usługodawcami	Zabezpiecz połączenia RDP zewnętrznych dostawców, partnerów i innych podmiotów łańcucha dostaw uzyskujących dostęp do Twojej infrastruktury IT.	Wdrażaj środki w celu wykrywania nieautoryzowanego dostępu do danych, eksfiltracji danych lub innych nietypowych zachowań użytkowników zdalnych stron trzecich.	Weryfikuj i zarządzaj tożsamościami członków łańcucha dostaw uzyskujących dostęp do Twojej infrastruktury.	Chroń dostęp do wrażliwych danych i krytycznych systemów, zapewniając dostawcom zewnętrznym jednorazowe hasła i ograniczając czas sesji użytkownika w infrastrukturze IT.	Przeprowadź ocenę ryzyka łańcucha dostaw poprzez wydanie kwestionariuszy i przeprowadzenie wizyt na miejscu z przedstawicielami łańcucha dostaw.	Określ oczekiwane wymogi bezpieczeństwa w umowach o gwarantowanym poziomie usług ze stronami trzecimi w celu zwiększenia odpowiedzialności.
Bezpieczeństwo nabywania, rozwijania i utrzymywania sieci i systemów informatycznych, w tym postępowanie z lukami w zabezpieczeniach i ich ujawnianie	Ogranicz dostęp do krytycznej infrastruktury programistycznej.	Monitoruj i rejestruj aktywności użytkowników w środowisku programistycznym w celu sprawdzenia, czy użytkownicy przestrzegają ustalonych zasad bezpieczeństwa.	Konfiguruj reguły w celu otrzymywania alertów o korzystaniu z podejrzanych aplikacji w środowisku programistycznym lub automatycznego wyłączania podejrzanych aplikacji.	Dokładnie oceniaj dostarczane oprogramowanie i usługi podczas procesu zakupu.	Ustanów proces zarządzania poprawkami i polityki ujawniania luk w zabezpieczeniach (VDP) w celu wyeliminowania pojawiających się słabych punktów.	Przyjmij standardy i praktyk kodowania w celu wyeliminowania zagrożeń bezpieczeństwa podczas tworzenia oprogramowania.
Zasady i procedury oceny skuteczności środków zarządzania ryzykiem cyberbezpieczeństwa	Monitoruj, w jaki sposób Twoi pracownicy i inni użytkownicy przestrzegają zasad bezpieczeństwa danych i innych zasad cyberbezpieczeństwa w Twojej organizacji.	Korzystaj z dzienników audytu aktywności użytkowników, aby ocenić, jak środki cyberbezpieczeństwa działają w Twojej organizacji.	Opracuj zasady określające sposób oceny środków zarządzania ryzykiem cyberbezpieczeństwa.	Zdefiniuj kluczowe wskaźniki wydajności, aby zmierzyć skuteczność określonych kontroli cyberbezpieczeństwa i wysiłków w zakresie zarządzania ryzykiem.	Przeprowadzaj regularne wewnętrzne i zewnętrzne audyty bezpieczeństwa, aby zidentyfikować luki i obszary wymagające poprawy.	Prowadź szczegółową dokumentację procesów oceny bezpieczeństwa, ustaleń i podjętych działań.
Podstawowe praktyki higieny cybernetycznej i szkolenia w zakresie cyberbezpieczeństwa	Uzyskaj wgląd w działania i zachowania użytkowników, aby zidentyfikować i rozwiązać wszelkie luki w podstawowych praktykach higieny cybernetycznej i wykryć naruszenia zasad.	Monitoruj działania użytkowników podczas testów penetracyjnych w celu dostarczania ukierunkowanych informacji zwrotnych użytkownikom i promowania przestrzegania najlepszych praktyk w zakresie cyberbezpieczeństwa.	Wykorzystaj nagrane sesje użytkowników do opracowywania materiałów i studiów przypadku na potrzeby inicjatyw szkoleniowych w zakresie świadomości cyberbezpieczeństwa.	Ukształtuj nawyki użytkowników w zakresie cyberbezpieczeństwa poprzez wyświetlanie komunikatów ostrzegawczych w odpowiedzi na niedozwolone działania.	Przeprowadzaj regularne szkolenia z zakresu cyberbezpieczeństwa obejmujące podstawowe praktyki cyberbezpieczeństwa, zagrożenia cybernetyczne i wektory ataków.	Uławtw współpracę między pracownikami, zespołem IT i ekspertami ds. bezpieczeństwa w celu dzielenia się wiedzą na temat cyberbezpieczeństwa i omawiania wszelkich pytań i wątpliwości dotyczących bezpieczeństwa.
Zasady i procedury dotyczące stosowania kryptografii i szyfrowania	Szyfruj dane monitorowania aktywności użytkowników, połączeń i innych poufnych rekordów.	Szyfruj hasła i sekrety użytkowników w swojej organizacji.	Szyfruj wszystkie nazwy użytkowników i aliasów podczas monitorowania aktywności użytkowników w celu ochrony prywatności użytkowników.	Szyfruj poufne pliki, bazy danych i systemy pamięci masowej.	Stwórz jasne zasady określające, które zasoby wymagają szyfrowania i jakich algorytmów używa Twoja organizacja.	Wdrażaj bezpieczne protokoły komunikacyjne, takie jak SSL i TLS, aby chronić dane podczas ich przesyłania.
Bezpieczeństwo zasobów ludzkich, zasady kontroli dostępu i zarządzanie zasobami	Zapewnij bezpieczeństwo zasobów ludzkich poprzez wykrywanie i badanie wszelkich nieautoryzowanych lub podejrzanych działań wykonywanych przez pracowników.	Kontroluj dostęp do zasobów wrażliwych i wdróż zasady najmniejszych uprawnień.	Rejestruj interakcje użytkowników z krytycznymi zasobami i systemami w celu zapewnienia śledzenia, rozliczalności i ochrony zasobów.	Prowadź kompleksową inwentaryzę wszystkich zasobów, w tym sprzętu i oprogramowania.	Przeprowadź kontrolę przeszłości kandydatów do pracy, aby upewnić się, że nie stanowią oni zagrożenia dla bezpieczeństwa.	Ustanów procedury dotyczące odejść pracowników, w tym cofania dostępu i zbierania zasobów firmy.
Bezpieczeństwo zasobów ludzkich, zasady kontroli dostępu i zarządzanie aktywami, stosowanie uwierzytelniania wieloskładnikowego lub rozwiązań ciągłego uwierzytelniania, zabezpieczonej komunikacji głosowej, wideo i tekstowej oraz zabezpieczonych systemów komunikacji awaryjnej jednostki, w stosownych przypadkach	Zmniejsz ryzyko nieautoryzowanego dostępu i naruszenia bezpieczeństwa konta za pomocą uwierzytelniania dwuskładnikowego.	Ustanów bezpieczny obieg wniosków o dostęp i zatwierdzeń oraz usprawnij procedury uwierzytelniania w organizacji.	Przejmij kontrolę nad hasłami swoich pracowników, wdrażając rozwiązania do zarządzania hasłami.	Zapewnij bezpieczną komunikację poprzez szyfrowanie wszystkich kanałów komunikacji, zwłaszcza w przypadku poufnych informacji.	Opracuj oddzielny, bezpieczny system komunikacji awaryjnej, taki jak dedykowana linia telefoniczna, telefon satelitarny lub specjalna aplikacja.	Przeszkol pracowników w zakresie bezpiecznych praktyk komunikacyjnych, takich jak rozpoznawanie prób phishingu i unikanie udostępniania poufnych informacji za pośrednictwem niezaszyfrowanych kanałów.

Legenda

Działania zapewnione przez Ekran System

- Monitoring aktywności użytkowników
- Zarządzanie uprzywilejowanym dostępem
- Nagrywanie sesji użytkownika
- Alerty aktywności
- Reagowanie na incydenty
- Badanie incydentów
- Audytowanie i raportowanie
- Zarządzanie hasłami
- Uwierzytelnianie wieloskładnikowe
- Zarządzanie tożsamością
- Monitorowanie sesji RDP
- Monitorowanie przez osoby trzecie
- Anonimizacja monitorowanych danych
- Eksport sesji użytkownika
- Szyfrowanie

Działania objęte innymi rozwiązaniami i środki organizacyjne

- Organizacyjne środki
- Inne rozwiązania