Ekran system

SECURIVY

EBOOK

Kompletny przewodnik po zgodności z NIS2

Spełnij wymagania dyrektywy krok po kroku

- Uzyskaj zgodność z wymaganiami NIS2
- Zabezpiecz swoje wrażliwe dane
- Zwiększ bezpieczeństwo Twojego łańcucha dostaw
- Uniknij grzywny i odpowiedzialności sądowej
- Zapewnij szybką reakcję na incydenty
- Zarządzaj zagrożeniami wewnętrznymi

www.ekransystem.com/pl | securivy.com

biuro@securivy.com

Wstęp

Wszystkie organizacje muszą być świadome stale zmieniających się przepisów i regulacji, aby chronić swoje wrażliwe aktywa i uniknąć płacenia milionowych kar. Szybki rozwój cyberzagrożeń napędzony przez globalną pandemię i cyberwojnę zmusił Unię Europejską (UE) do aktualizacji dyrektywy NIS.

Jesteśmy świadomi trudności, związanej z koniecznością czytania setek wymogów i regulacji prawnych oraz innych dokumentów, więc zrobiliśmy to za Ciebie. Ten ebook pomoże ci zorganizować proces uzyskania zgodności z NIS2 i dostarczy listę najlepszych praktyk, które pozwolą przygotować Twoją organizację z wyprzedzeniem.

Zbadamy również, w jaki sposób bogate w funkcje rozwiązania, takie jak Ekran System, mogą pomóc w spełnieniu wymagań NIS2.

Ekran System to kompleksowa platforma do zarządzania ryzykiem wewnętrznym, która oferuje holistyczne podejście do zarządzania cyberbezpieczeństwem na poziomie użytkownika. Dzięki Ekran System możesz monitorować aktywność użytkowników, zarządzać dostępem i reagować na zagrożenia bezpieczeństwa.

Spis treści

Czym jest dyrektywa NIS2

Co to jest dyrektywa NIS2?

NIS2, czyli dyrektywa (EU) 2022/2555, ma na celu podniesienie ogólnego poziomu cyberbezpieczeństwa w Unii Europejskiej i zapewnienie odporności sieci i systemów informatycznych infrastruktury krytycznej działającej w regionie.

> Państwa członkowskie zapewniają, aby podmioty kluczowe i ważne wprowadzały odpowiednie i proporcjonalne środki techniczne, operacyjne i organizacyjne w celu zarządzania ryzykiem dla bezpieczeństwa sieci i systemów informatycznych wykorzystywanych przez te podmioty do prowadzenia działalności lub świadczenia usług oraz w celu zapobiegania wpływowi incydentów na odbiorców ich usług lub na inne usługi bądź minimalizowania takiego wpływu.
>
> Dyrektywa NIS2, Artykuł 21

Co nowego w dyrektywie NIS2?

Dyrektywa w sprawie środków na rzecz wysokiego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii Europejskiej (NIS) została ustanowiona w lipcu 2016 r. w celu wspierania współpracy i zwiększenia cyberbezpieczeństwa organizacji działających w Unii Europejskiej (UE) na poziomie krajowym.

NIS2 wszedł w życie w styczniu 2023 r., obejmując szerszy zakres i wprowadzając dodatkowe wymogi, obowiązki sprawozdawcze i sankcje w odpowiedzi na zwiększoną częstotliwość i wpływ cyberataków na infrastrukturę krytyczną UE w ostatnim czasie.

Kluczowe obszar wymagań NIS2

- Ocena oraz zarządzanie ryzykiem
- Integralność danych
- Zarządzanie oraz raportowanie incydentów
- Ciągłość działania
- Bezpieczeństwo systemów IT
- Bezpieczeństwo łańcucha dostaw

Kogo dotyczy dyrektywa NIS2?

Dyrektywa NIS2 ma zastosowanie dla następujących podmiotów funkcjonujących na terenie Unii Europejskiej:

Kluczowe podmioty lub podmioty działające w sektorach o wysokim stopniu krytyczności

- Sektor energetyczny
- Transport
- Rynki finansowe
- Bankowość
- Opieka zdrowotna
- Dystrybucja wody pitnej
- Oczyszczalnie ścieków
- infrastruktura cyfrowa
- Zarządzanie usługami ICT (B2B)
- Administracja publiczna
- Przemysł kosmiczny

Ważne podmioty lub podmioty działające w innych krytycznych sektorach

- Usługi pocztowe i kurierskie
- Gospodarowanie odpadami
- Produkcja, wytwarzanie i dystrybucja chemikaliów
- Produkcja, przetwarzanie i dystrybucja żywności
- Przemysł
- Dostawcy usług cyfrowych
- Organizacje badawcze

Uwaga: Więcej informacji na temat sektorów i organizacji, których dotyczy dyrektywa, można znaleźć w art. 2 dyrektywy NIS2 oraz w załącznikach I i II do tej dyrektywy.

Czy Twoja organizacja powinna przejmować się NIS2, jeśli znajduje się poza UE?

Dyrektywa NIS2 ma zastosowanie do każdego podmiotu świadczącego usługi krytyczne w krajach Unii Europejskiej, **niezależnie od jego geograficznej lokalizacji**. Tak więc nawet jeśli Twoja organizacja nie jest fizycznie zlokalizowana w UE, nadal może podlegać NIS2.

Terminy	Konsekwencje nieprzestrzegania przepisów
NIS2 wymaga od wszystkich państw członkowskich włączenia jej do prawa krajowego do **17 października 2024 roku.** Każdy kraj UE będzie również musiał zidentyfikować i zarejestrować wszystkie istotne i ważne podmioty do **17 kwietnia 2025 r.**	• Grzywny w wysokości do 10 milionów euro lub co najmniej 2% całkowitego rocznego światowego obrotu w przypadku podmiotów kluczowych • Grzywny w wysokości do 7 milionów euro lub co najmniej 1,4% całkowitego rocznego światowego obrotu w przypadku podmiotów ważnych. • Sankcje wobec menedżerów najwyższego szczebla. • Zawieszenie certyfikatów i zezwoleń na usługi świadczone przez organizację.

Przygotowanie do uzyskania zgodności z NIS2

Przygotowanie jest kluczowe, ponieważ wyposaża Twoją organizację w niezbędną wiedzę, aby sprostać rozszerzonemu zakresowi NIS2. Etap ten pomoże odpowiednio zaplanować działania i stworzyć skuteczną strategię osiągnięcia celów w zakresie zgodności.

1. Zrozum zakres

Ustalenie zakresu NIS2, które spośród Twoich systemów OT/IT wchodzą w jej zakres oraz jakie komplikacje dyrektywa może mieć dla Twojej organizacji, jest pierwszym krokiem do uzyskania zgodności. Rozważ następujące pytania:

- Jakie podstawowe usługi świadczy Twoja organizacja?
- Czy Twoją organizację można uznać za kluczowy lub ważny podmiot?
- Jakie nowe środki bezpieczeństwa może wdrożyć Twoja organizacja, aby zapewnić zgodność z przepisami?
- Czy masz dostawców, partnerów lub klientów podlegających dyrektywie?
- Czy w umowach kontraktowych z dostawcami i partnerami należy uwzględnić nowe zobowiązania dotyczące zgodności z NIS2?

Uwaga: Jeśli Twoja organizacja należy do sektorów krytycznych zdefiniowanych przez NIS2, ważne jest również, aby wziąć pod uwagę wielkość organizacji, ponieważ tylko średnie i duże przedsiębiorstwa podlegają NIS2.

Progi wielkości dla istotnych i ważnych podmiotów podlegających NIS2			
	Liczba pracowników	**Roczny obrót**	**Podlega NIS2**
Duże przedsiębiorstwo	250 lub więcej	Ponad 50 milionów euro	✓
Średnie przedsiębiorstwo	50 lub więcej	Ponad 10 milionów euro	✓
Małe przedsiębiorstwo	Mniej niż 50	Mniej niż 10 milionów euro	–

Rekomendacja 2003/361/EC

Organizacje zatrudniające mniej niż 50 pracowników lub mające roczny obrót poniżej 10 milionów euro nie podlegają przepisom NIS2, chyba że zostaną uznane za organizacje o krytycznym znaczeniu dla społeczeństwa. Artykuł 2 dyrektywy zawiera również listę innych wyjątków, niezależnie od wielkości podmiotu.

2. Zapoznaj się z wymaganiami bezpieczeństwa NIS2

Artykuł 21 dyrektywy określa główne wymogi NIS2, z których większość koncentruje się na środkach zapewniających bezpieczeństwo organizacyjne. Identyfikacja i zrozumienie tych środków jest kluczowe dla zapewnienia zgodności.

Zgodnie z NIS2 podmioty muszą wdrożyć następujące 10 środków w celu "zarządzania ryzykiem dla bezpieczeństwa sieci i systemów informatycznych" wykorzystywanych do świadczenia ich podstawowych i ważnych usług:

01 Polityki analizy ryzyka i bezpieczeństwa systemów informatycznych;

02 Obsługa incydentu;

03 Ciągłość działania, np. zarządzanie kopiami zapasowymi i przywracanie normalnego działania po wystąpieniu sytuacji nadzwyczajnej, i zarządzanie kryzysowe;

04 Bezpieczeństwo łańcucha dostaw, w tym aspekty związane z bezpieczeństwem dotyczące stosunków między każdym podmiotem a jego bezpośrednimi dostawcami lub usługodawcami;

05 Bezpieczeństwo w procesie nabywania, rozwoju i utrzymania sieci i systemów informatycznych, w tym postępowanie w przypadku podatności i ich ujawnianie;

06 Polityki i procedury służące ocenie skuteczności środków zarządzania ryzykiem w cyberbezpieczeństwie;

07 Podstawowe praktyki cyberhigieny i szkolenia w zakresie cyberbezpieczeństwa;

08 Polityki i procedury stosowania kryptografii i, w stosownych przypadkach, szyfrowania;

09 Bezpieczeństwo zasobów ludzkich, politykę kontroli dostępu i zarządzanie aktywami;

10 W stosownych przypadkach – stosowanie uwierzytelniania wieloskładnikowego lub ciągłego, zabezpieczonych połączeń głosowych, tekstowych i wideo oraz zabezpieczonych systemów łączności wewnątrz podmiotu w sytuacjach nadzwyczajnych.

3. Przeprowadź analizę luk

Po zidentyfikowaniu zakresu i wymagań NIS2, jesteś gotowy, aby porównać je z istniejącymi środkami bezpieczeństwa wdrożonymi w Twojej organizacji. Analiza ta niweluje wszelkie istniejące luki między obecnym stanem zgodności a pożądanym, aby dostosować Twoją organizację do wymagań narzucanych przez NIS2.

Korzyści z wykonania analizy luk

Aby przeprowadzić właściwą analizę luk, należy wykonać następujące kluczowe kroki:

1. **Zdefiniowanie wymagań i zakresu analizy luk.** Skomponuj deklarację zakresu określające procesy, systemy, polityki i osoby, które będą oceniane.
2. **Określ pożądane poziomy odniesienia**. Zdefiniuj idealny stan zgodności, który organizacja chce osiągnąć.
3. **Oceń aktualny stan cyberbezpieczeństwa.** Oceń i udokumentuj istniejące polityki, procedury i mechanizmy kontroli w zakresie cyberbezpieczeństwa.
4. **Porównaj istniejące mechanizmy kontrolne z wymaganymi.** Porównanie istniejących środków i polityk cyberbezpieczeństwa z wymogami NIS2.
5. **Zidentyfikuj luki w zgodności.** Wskaż obszary, w których obecny stan cyberbezpieczeństwa jest niewystarczający.
6. **Określ poziom dotkliwości i wpływu zidentyfikowanych luk zgodności.**
7. **Opracuj plan działania.** W oparciu o zidentyfikowane luki i ustalone punkty odniesienia, utwórz szczegółowy plan działania z jasnymi celami i terminami, który obejmie wszystkie luki w zakresie zgodności.

Rozważ regularne przeprowadzanie analizy luk, aby nadążyć za stale zmieniającymi się wymogami cyberbezpieczeństwa i zidentyfikować potencjalne zagrożenia.

4. Przydziel niezbędne zasoby

Pomyślne wdrożenie wymogów dyrektywy NIS2 wiąże się z przydzieleniem potrzebnych zasobów, w tym pieniędzy, ludzi i technologii.

Oszacuj budżet na działania związane z uzyskaniem zgodności

Przydziel odpowiedzialnych pracowników

Zainwestuj w technologie bezpieczeństwa

Oszacuj budżet na działania związane z uzyskaniem zgodności. Planowanie wydatków pomoże uzyskać zgodę osób decyzyjnych oraz pozwoli uniknąć nieoczekiwanych kosztów.

Nie ma jednego uniwersalnego scenariusza planowania wzrostu wydatków, ponieważ różnią się one w zależności od zaimplementowanych w organizacji zabezpieczeń. Raport Impact Assessment Report 1/3 szacuje, że średnie wydatki na bezpieczeństwo systemów ICT wzrosną o około 12% do 22%.

Szacowany przeciętny wzrost wydatków na bezpieczeństwo systemów ICT w sektorach podlegających dyrektywie NIS2

12% - sektory podlegające poprzedniej dyrektywie NIS

22% - nowe sektory włączone w zakres obowiązywania NIS2

Przydziel odpowiedzialnych pracowników. Ten krok obejmuje zebranie zespołu ekspertów ds. cyberbezpieczeństwa odpowiedzialnych za uzyskanie zgodności. Taki zespół może obejmować analityków bezpieczeństwa, inspektorów ds. zgodności oraz profesjonalistów IT. Jasno określ obowiązki każdego członka zespołu, upewniając się, że każdy rozumie swoją rolę.

Dla uzyskania najlepszego efektu, poszukaj pomocy pośród film specjalizujących się w zapewnianiu zgodności z NIS2. Zewnętrzni eksperci mogą poszerzyć Twoją wiedzę na temat wymagań dyrektywy NIS2 oraz metodologii jej efektywnego wdrażania.

Zainwestuj w technologie bezpieczeństwa. Sprawdź, które rozwiązania technologiczne mogą pomóc Ci wypełnić luki, które zostały zidentyfikowane podczas analizy luk. Możesz również rozważyć narzędzia automatyzacji, które mogą usprawnić procesy zgodności i zmniejszyć obciążenie pracą manualną.

Aby zmniejszyć obciążenie finansowe związane z wdrażaniem technologii bezpieczeństwa, możesz ubiegać się o pomoc finansową od organizacji takich jak Program “Cyfrowa Europa”, które finansują różne cyfrowe inicjatywy.

5. Zaangażuj osoby zarządzające organizacją

Sukces każdej inicjatywy w zakresie uzyskania zgodności zależy od wsparcia liderów organizacji. Osoby zarządzające muszą być świadome potrzeb organizacji w zakresie zapewnienia bezpieczeństwa na najwyższym poziomie, ponieważ odgrywają one kluczową rolę w zapewnieniu zgodności z NIS2.

01 Poinformuj zarząd o karach przewidzianych za brak zgodności z dyrektywą NIS2

02 Przeszkól kadrę zarządzającą o ryzykach związanych z cyberbezpieczeństwem i zarządzaniu nimi.

03 Szukaj wsparcia pośród osób zarządzających

Przede wszystkim należy poinformować zarząd o karach opisanych w dyrektywie NIS2. Oprócz wspomnianych kar, NIS2 szczegółowo określa odpowiedzialność "organów zarządzających" za naruszenia wymogów zarządzania ryzykiem w zakresie cyberbezpieczeństwa i obowiązków sprawozdawczych wynikających z dyrektywy.

Sankcje przewidywane w przypadku nieprzestrzegania NIS2

- Podanie do informacji publicznej danych osób odpowiedzialnych za złamanie dyrektywy oraz szczegółów nieprzestrzegania jej przez organizację
- Zakaz pełnienia funkcji zarządczych dla każdej osoby decyzyjnej odpowiedzialnej za naruszenia
- Zawieszenie certyfikowania i autoryzacji dla wykonywania usług świadczonych przez organizację

Ważne jest również, aby wyraźnie informować o znaczeniu zgodności z NIS2 w innych aspektach organizacji, w tym w zakresie ochrony reputacji, bezpieczeństwa danych i ogólnej ciągłości działalności biznesowej.

Edukacja kadry kierowniczej wyższego szczebla w zakresie zarządzania ryzykiem cyberbezpieczeństwa. Przeprowadzenie **sesji edukacyjnych** z zarządem w celu lepszego zrozumienia kwestii cyberbezpieczeństwa, wymagań cyberbezpieczeństwa NIS2 i obecnego stanu cyberbezpieczeństwa organizacji.

Spis treści →

Artykuł 20. Dyrektywy NIS2 wymaga od kadry zarządzającej organizacją:

- **Zatwierdzania środków zarządzania ryzykiem** z zakresu cyberbezpieczeństwa i nadzorowanie ich wdrażania

- **Odbywanie szkoleń** i regularne oferowanie pracownikom podobnych szkoleń w celu "[zdobycia] wystarczającej wiedzy i umiejętności, aby umożliwić im identyfikację zagrożeń i ocenę praktyk zarządzania ryzykiem z zakresu cyberbezpieczeństwa".

Szukaj wsparcia wśród osób zarządzających. Znajdź osobę na stanowisku kierowniczym, która będzie wspierać Twoje inicjatywy w zakresie cyberbezpieczeństwa, promować wysiłki na rzecz zgodności z NIS2 i zabiegać o niezbędne zasoby.

Szukając takiej osoby, priorytetowo traktuj tych, którzy rozumieją znaczenie technologii, stawiają wyniki ponad zasadami oraz są gotowi zainwestować czas i wysiłek w te działania. Współpraca z taką osobą pozwala dostosować działania do oczekiwań zarządu i przyspieszyć procesy związane z zapewnianiem zgodności.

Wskazówki dotyczące wdrażania wymagań NIS2

W tej sekcji dokonujemy przeglądu dziesięciu wymogów zarządzania ryzykiem z zakresu cyberbezpieczeństwa przedstawionych w dyrektywie NIS2 i przedstawiamy praktyczne wskazówki dotyczące ich wdrażania.

Wymóg 1.

Analiza ryzyka i bezpieczeństwa systemów informatycznych

Wymóg ten mówi, że organizacje muszą ustanowić jasne zasady i procedury oceny ryzyka w zakresie cyberbezpieczeństwa i zarządzania nim. Aby spełnić ten wymóg, należy rozważyć:

Wdrożenie zasad oceny ryzyka. Należy opracować procedury identyfikacji, oceny i priorytetyzacji zagrożeń z zakresu cyberbezpieczeństwa w organizacji. Obejmuje to ocenę potencjalnych zagrożeń, słabych punktów i wpływu incydentów na systemy informatyczne. Procedury te można udokumentować i sformalizować, opracowując zasady analizy ryzyka, które określają zakres, metodologie i częstotliwość ocen ryzyka.

Najczęstsze pytania zadawane podczas oceny ryzyka cyberbezpieczeństwa:

- Jakie ryzyka w zakresie bezpieczeństwa oraz słabe punkty istnieją w Twoim środowisku IT?
- Jakie jest prawdopodobieństwo wystąpienia incydentu bezpieczeństwa?
- Jakie konsekwencje może pociągnąć za sobą incydent?
- Jak poważne są ryzyka bezpieczeństwa wedle priorytetów?
- Jak można złagodzić potencjalne zagrożenia?

Ustanów polityki bezpieczeństwa systemów informacyjnych. Solidne polityki cyberbezpieczeństwa pozwalają na określenie jasnych zasad dotyczących danych i bezpieczeństwa systemów, wprowadzenie odpowiednich kontroli cyberbezpieczeństwa oraz poprawę efektywności operacyjnej. Posiadanie jasnych polityk pozwala na standaryzację i synchronizację działań związanych z bezpieczeństwem w całej organizacji, zapewniając, że wszyscy działają zgodnie z tymi samymi wytycznymi.

Kluczowe aspekty polityk bezpieczeństwa systemów informacyjnych:

Zamiast opracowywania różnorodnych polityk związanych z bezpieczeństwem, rozważ wdrożenie kompleksowego systemu zarządzania bezpieczeństwem informacji (ISMS), który pomaga zmniejszyć ryzyko cyfrowe dzięki systemowemu podejściu. Możesz użyć ISO 27001 oraz rekomendacji ENISA jako fundamentu dla stworzenia ISMS.

Spis treści →

Wymóg 2.

Obsługa incydentów i raportowanie

Organizacje podlegające dyrektywie NIS2 muszą posiadać procedury postępowania i raportowania incydentów z zakresu cyberbezpieczeństwa. Rozważ podjęcie działań:

Zaplanuj swoją odpowiedź na incydenty. Opracuj kompleksowy plan reagowania na incydenty (IRP), określający kroki, które należy podjąć w przypadku różnych typów incydentów cyberbezpieczeństwa. IRP (Incident Response Plan) zapewnia osobom odpowiedzialnym za bezpieczeństwo konkretne wytyczne i pewność do szybkiego działania w zakresie wykrywania i reagowania na zagrożenia bezpieczeństwa.

Kluczowe etapy postępowania z incydentami cyberbezpieczeństwa według NIST

Zgodnie z NIST800-61

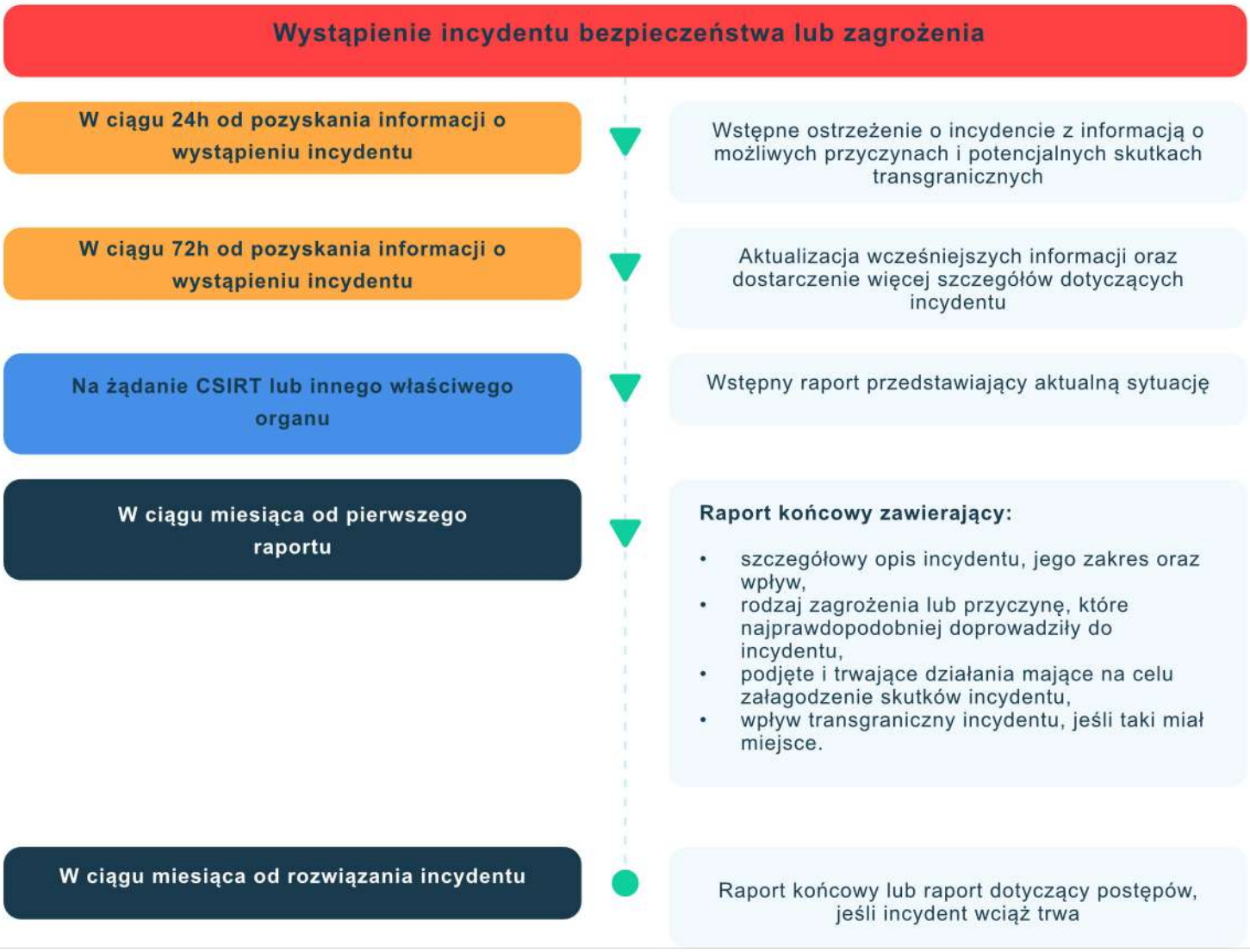
Rozważ przygotowanie planu reagowania na incydenty zgodnie z przewodnikiem "Computer Security Incident Handling Guide, 800-61 Revision 2" opracowanym przez National Institute of Standards and Technology (NIST).

Dokumentuj raportowane incydenty. Ponieważ NIS2 wymaga od organizacji spełnienia ścisłych obowiązków sprawozdawczych, dodaj je do swojego programu reagowania na incydenty.

Zgodnie z Artykułem 23 dyrektywy, podmioty kluczowe i ważne muszą powiadomić odpowiednie jednostki w przypadku wystąpienia incydentu bezpieczeństwa:

- Narodowe Zespoły Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT) lub inne właściwe organy państw członkowskich, w Polsce jest to NASK CSIRT
- Odbiorców usług, jeśli incydent może negatywnie wpłynąć na świadczenie tych usług (w odpowiednich przypadkach)
- Podmioty dotknięte istotnym zagrożeniem (w odpowiednich przypadkach)

Wymogi czasowe w zakresie raportowania zgodnie z NIS2



Wymóg 3.

Zapewnienie ciągłości działalności poprzez zarządzanie kopiami zapasowymi, odzyskiwanie danych po awariach i zarządzanie kryzysowe

To wymaganie podkreśla istotną wagę zapewnienia odporności systemów informacyjnych oraz całości organizacji. Aby sprostać temu wymogowi, rozważ podjęcie następujących działań:

Typowe praktyki mające na celu zapewnienie ciągłości działania organizacji:

- Wprowadzenie regularnych procedur tworzenia kopii zapasowych dla krytycznych danych i systemów.
- Nakreślenie sposobów odzyskiwania danych oraz systemów w akceptowalnych ramach czasowych.
- Utworzenie dedykowanego zespołu zarządzania kryzysowego odpowiedzialnego za koordynowanie reakcji na incydenty.

Ustanów dokładny plan zapewnienia ciągłości działalności (BCP), który zawiera postanowienia dotyczące zarządzania kopiami zapasowymi, odzyskiwania po awariach i zarządzania kryzysowego. BCP (Business Continuity Plan) określa procedury mające na celu zapewnienie ciągłej dostępności krytycznych usług i danych w obliczu incydentów cyberbezpieczeństwa i zakłóceń w pracy.

> *Planowanie ciągłości działalności to wszechstronne podejście do odzyskiwania działalności po wypadkach, który zakłada, że organizacje planują odzyskanie całego procesu działalności. Plan powinien obejmować miejsca pracy, telefony, stacje robocze, serwery, aplikacje, połączenia sieciowe i wszelkich inne zasoby niezbędne do prowadzenia działalności.*
>
> **Gartner**

Możesz rozpocząć od przeprowadzenia oceny ryzyka i obliczenia potencjalnych strat w przypadku różnych incydentów bezpieczeństwa. Następnie zacznij opracowywać swój BCP, postępując zgodnie z poniższymi krokami:

Kluczowe kroki w opracowywaniu planu ciągłości działania biznesu:

01 Określ zakres swojego BCP.

02 Zidentyfikuj kluczowe obszary biznesowe, funkcje krytyczne i zależności między nimi.

03 Określ akceptowalny czas przestoju dla każdej krytycznej funkcji działalności.

04 Opracuj plan utrzymania działalności organizacji.

Wymóg 4.

Bezpieczeństwo łańcucha dostaw, włączając w to aspekty związane z bezpieczeństwem dotyczące relacji między każdą jednostką a jej bezpośrednimi dostawcami lub usługodawcami

Nawet organizacje, które nie są bezpośrednio włączone w zakres dyrektywy, ale świadczą usługi dla podmiotów objętych NIS2, muszą zadbać o odpowiedni poziom cyberbezpieczeństwa.

> *Podmioty kluczowe i ważne powinny oceniać i uwzględniać ogólną jakość i odporność produktów i usług oraz środków zarządzania ryzykiem w cyberbezpieczeństwie stanowiący ich część, a także praktyki dotyczące cyberbezpieczeństwa stosowane przez dostawców produktów i usług, w tym ich procedury bezpiecznego opracowywania.*

Zarządzanie ryzykiem bezpieczeństwa w łańcuchu dostaw obejmuje:

Przeprowadzenie oceny ryzyka, zrozumienie poziomu cyberbezpieczeństwa dostawców, identyfikację podatności i potencjalnych zagrożeń. Warto wykorzystać kwestionariusze i wizytacje w celu oceny środków bezpieczeństwa.

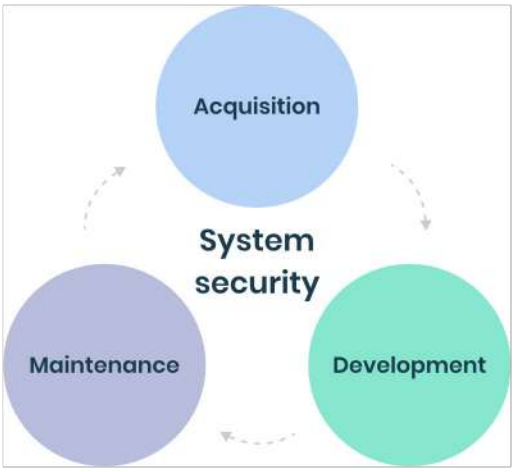
Współpracę z dostawcami, w tym ciągłą komunikację, organizowanie wydarzeń na rzecz odporności łańcucha dostaw, prowadzenie sesji szkoleniowych i promowanie świadomości. Aby zapewnić odpowiedzialność, można określić oczekiwania dotyczące bezpieczeństwa w umowach SLA z podmiotami trzecimi.

Ograniczenie dostępu podmiotów trzecich do systemów IT, stosowanie zasady najmniejszych uprawnień, jest kluczowe dla zapobiegania zagrożeniom wewnętrznym i atakom na łańcuch dostaw.

Wymóg 5.

Bezpieczeństwo w pozyskiwaniu, rozwoju i utrzymaniu systemów sieciowych i informacyjnych, w tym zarządzanie podatnościami i ich wykrywanie

Aby spełnić ten wymóg, rozważ zabezpieczenie systemów IT na każdym etapie ich cyklu życia. Celem jest zapewnienie, by system informacyjny był chroniony przez cały czas, minimalizując podatności i ryzyko. Gwarantowanie takiej ochrony wymaga wdrożenia odpowiednich środków:



Zabezpiecz proces pozyskiwania. Przy wyborze dostawców oprogramowania dokładnie oceniaj dostarczane produkty i usługi. Ponadto, jasno określ swoje wymagania bezpieczeństwa w umowach z podmiotami trzecimi, aby upewnić się, że są one zgodne z Twoimi wewnętrznymi politykami.

Aktualizuj systemy. Ustanów solidny proces zarządzania aktualizacjami, aby radzić sobie z pojawiającymi się podatnościami poprzez regularne aktualizacje oprogramowania.

Wprowadź bezpieczeństwo w procesie rozwoju. Przyjmij standardy i praktyki programowania w celu wyeliminowania ryzyka bezpieczeństwa podczas rozwoju oprogramowania zarówno z Twojej strony, jak i dostawców usług zewnętrznych.

Wdrożenie ciągłego monitoringu. Zastosuj mechanizmy monitorowania w celu ciągłego śledzenia i rejestrowania aktywności w sieciach i infrastrukturze IT. Oprogramowanie do monitorowania aktywności pozwala na wykrywanie i reagowanie na incydenty bezpieczeństwa w czasie rzeczywistym.

Rozwijanie procesu ujawniania słabości systemów. Ustanów politykę ujawniania podatności (VDP), aby zachęcać i ułatwiać odpowiedzialne zgłaszanie słabych punktów bezpieczeństwa w systemach, aplikacjach i sieciach.

> *Skoordynowane ujawnianie podatności to ustrukturyzowany proces, w ramach którego podatności są zgłaszane producentowi lub dostawcy potencjalnie podatnych produktów ICT lub usług ICT w sposób umożliwiający im zdiagnozowanie i wyeliminowanie danej podatności, zanim dotyczące jej szczegółowe informacje zostaną ujawnione osobom trzecim lub podane do wiadomości publicznej.*

Wymóg 6.

Polityki i procedury oceny skuteczności środków zarządzania ryzykiem cyberbezpieczeństwa.

Polityki i procedury oceny skuteczności środków zarządzania ryzykiem cyberbezpieczeństwa.

Dyrektywa NIS2 zobowiązuje organizacje do stworzenia uporządkowanego procesu weryfikacji skuteczności wdrożonych środków cyberbezpieczeństwa. Oto działania, które można podjąć:

Ustanów politykę oceny bezpieczeństwa. Opracuj klarowne i kompleksowe zasady określające metodykę oceny środków zarządzania ryzykiem cybernetycznym. Zdefiniuj również kluczowe wskaźniki wydajności mierzące efektywność określonych kontroli cyberbezpieczeństwa i ogólnych działań związanych z zarządzaniem ryzykiem.

Zaplanuj regularne przeglądy bezpieczeństwa. Przeprowadzaj wewnętrzne i zewnętrzne audyty bezpieczeństwa, aby identyfikować luki i obszary wymagające poprawy w politykach i standardach, tak by zapewnić zgodność z dyrektywą NIS2.

Najczęstsze pytania dotyczące oceny ryzyka cyberbezpieczeństwa:

- W jaki sposób nasza organizacja wykrywa podatności?
- Jak skuteczne są nasze środki zarządzania dostępem użytkowników?
- Czy nasze wrażliwe dane są odpowiednio chronione przed zagrożeniami wewnętrznymi i atakami zewnętrznymi?
- Czy mamy wgląd w ruch sieciowy i aktywność użytkowników?
- Czy możemy skutecznie ocenić środki bezpieczeństwa naszych dostawców zewnętrznych i partnerów?
- Jak dobrze pracownicy przestrzegają ustalonych polityk bezpieczeństwa?
- Jak szybko nasza organizacja może wykryć incydenty cyberbezpieczeństwa?
- Jaki jest średni czas potrzebny nam na opanowanie incydentu bezpieczeństwa?

Dokumentuj audyty bezpieczeństwa. Utrzymuj szczegółową dokumentację swoich procesów oceny bezpieczeństwa, wyników oraz podjętych działań. Takie zapisy mogą przyspieszyć przyszłe audyty oraz służyć jako potwierdzenie przestrzegania dyrektywy NIS2 wobec zewnętrznych audytorów i organów regulacyjnych.

Wymóg 7.

Podstawowe praktyki cyberhigieny i szkolenia z zakresu cyberbezpieczeństwa

Dyrektywa NIS2 podkreśla potrzebę podstawowych działań mających na celu zwiększenie świadomości z zakresu cyberbezpieczeństwa i praktyk higieny cybernetycznej wśród Twoich pracowników. Rozważ wykonanie następujących działań w tym zakresie:

Edukuj swoich pracowników. Przeprowadzaj regularne szkolenia z zakresu cyberbezpieczeństwa, obejmujące podstawowe praktyki cyberbezpieczeństwa i edukuj pracowników na temat powszechnych zagrożeń cybernetycznych i wektorów ataków.

Ułatwiaj współpracę. Stwórz środowisko, w którym Twoi pracownicy, zespół IT i eksperci ds. bezpieczeństwa są chętni do dzielenia się swoją wiedzą z zakresu cyberbezpieczeństwa i omawiania swoich pytań i obaw dotyczących bezpieczeństwa.

Twoim ostatecznym celem jest stworzenie kultury cyberbezpieczeństwa, w której bezpieczeństwo jest zintegrowane z każdym aspektem działania Twojej organizacji, poprawiając kolektywną świadomość i zaangażowanie w łagodzenie ryzyka cyberbezpieczeństwa.

Tematy do szkolenia z zakresu cyberbezpieczeństwa

- Bezpieczeństwo haseł
- Świadomość inżynierii społecznej
- Bezpieczne praktyki surfowania w Internecie
- Bezpieczeństwo urządzeń
- Bezpieczeństwo pracy zdalnej
- Raportowanie incydentów

Wymóg 8.

Polityki i procedury dotyczące stosowania kryptografii i szyfrowania

Organizacje mogą spełnić to wymaganie, implementując polityki dotyczące stosowania szyfrowania i zapewniając ochronę wrażliwych informacji podczas ich transmisji:

Stwórz jasne polityki określające, które zasoby wymagają szyfrowania i jakie algorytmy stosuje firma.

Chroń swoje dane przed nieautoryzowanym dostępem poprzez szyfrowanie wrażliwych plików, baz danych i innych systemów przechowywania. Wdrażaj bezpieczne protokoły komunikacyjne, takie jak SSL i TLS, aby chronić Twoje dane w trakcie transmisji.

Powszechne zastosowania szyfrowania:

- Przechowywanie danych i ich transmisja
- E-maile i aplikacje do wysyłania wiadomości
- Anonimizacja danych
- Uwierzytelnianie użytkowników i haseł
- Bezpieczeństwo w chmurze

Wymóg 9.

Bezpieczeństwo zasobów ludzkich, polityki kontroli dostępu i zarządzanie zasobami.

Organizacje podlegające NIS2 muszą wdrożyć odpowiednie środki do kontroli dostępu użytkowników, bezpiecznego zarządzania zasobami i zmniejszenia ryzyka związanego z ludźmi i Twoimi wrażliwymi zasobami. Aby spełnić to wymaganie, rozważ następujące kluczowe praktyki:

Przejrzyj swoje procesy onboardingu i zakończenia współpracy. Jednym z kluczowych celów bezpieczeństwa zasobów ludzkich jest zapewnienie, że osoby mające dostęp do wrażliwych informacji są godne zaufania. Rozważ przeprowadzenie kontroli kandydatów do pracy, aby upewnić się, że nie stanowią zagrożenia dla bezpieczeństwa. Ustal również procedury na wypadek odejścia pracowników, w tym cofania dostępów i odzyskiwania zasobów firmy.

Zarządzaj dostępem użytkowników. Efektywne zarządzanie uprawnieniami dostępu użytkowników jest kluczem do zapobiegania nieautoryzowanemu dostępowi i eliminowania niepotrzebnych ryzyk. Rozważ opracowanie swoich polityk kontroli dostępu wokół idei ograniczania uprawnień dostępu użytkowników.

Efektywne metody ograniczania dostępu użytkownikom:

Podejście "just-in-time"

Przyznawaj użytkownikom dostęp do kont i zasobów tylko na ograniczony czas i z ważnego powodu.

Zasada najmniejszych uprawnień (PoLP)

Przyznawaj użytkownikom dostęp tylko do zasobów niezbędnych do wykonywania bezpośrednich obowiązków służbowych.

Model "Zero-trust"

Nigdy nie ufaj użytkownikom i urządzeniom w swojej infrastrukturze oraz poza nią i zawsze weryfikuj tożsamość użytkowników.

Zwiększ widoczność i kontrolę nad wrażliwymi zasobami. Utrzymuj kompleksowy inwentarz wszystkich zasobów, w tym sprzętu i oprogramowania. Znając lokalizację i wartość swoich zasobów, Twoja organizacja może lepiej chronić je przed kradzieżą, utratą lub uszkodzeniem.

Ponadto, **wdróż rozwiązanie do ciągłego monitorowania aktywności użytkowników**, aby uzyskać informacje w czasie rzeczywistym o tym, jak użytkownicy uzyskują dostęp do Twoich zasobów i jak ich używają. Możesz wykorzystać te informacje do identyfikacji podejrzanej aktywności, problemów zgodności i innych sytuacji.

Kluczowe korzyści z monitorowania aktywności użytkowników:

- ✓ Zwiększenie widoczności systemu
- ✓ Ochrona wrażliwych danych
- ✓ Wykrywanie zagrożeń bezpieczeństwa
- ✓ Nadzór nad wdrażaniem polityk bezpieczeństwa

Wymóg 10.

Wykorzystaj wieloskładnikowe uwierzytelnianie lub uwierzytelnianie ciągłe

Wprowadzenie wieloskładnikowego uwierzytelniania (MFA) i ciągłych rozwiązań uwierzytelniania pozwala na zapobieganie nieautoryzowanemu dostępowi, zmniejszenie ryzyka kompromitacji konta i zwiększenie ogólnego bezpieczeństwa sieci i systemów.

MFA i ciągłe uwierzytelnianie to metody uwierzytelniania, które wykraczają poza tradycyjną kombinację nazwy użytkownika i hasła, aby zweryfikować tożsamość użytkownika przed udzieleniem mu dostępu oraz uprawnień do twojego systemu przedsiębiorstwa.

Zastosuj MFA do swoich kluczowych zasobów. MFA zazwyczaj wymaga od użytkowników podania dwóch lub więcej elementów uwierzytelniania, takich jak hasło, token bezpieczeństwa lub biometryczny identyfikator, w celu dostępu do systemu lub zasobu. Rozważ priorytetowe użycie MFA do dostępu do kluczowych systemów i wrażliwych danych i upewnij się, że edukujesz użytkowników, jak prawidłowo korzystać z MFA.

Wdróż kompleksowe rozwiązania uwierzytelniania. Zarządzanie tożsamością i dostępem (IAM) oraz zarządzanie dostępem uprzywilejowanym (PAM) mogą zapewnić twojej organizacji scentralizowaną kontrolę nad uwierzytelnianiem użytkowników i uprawnieniami dostępu. Takie rozwiązania przyczyniają się do wdrożenia zasady najmniejszych uprawnień w twojej organizacji. Ciągłe uwierzytelnianie idzie o krok dalej, stale weryfikując tożsamość użytkownika podczas aktywnej sesji.

Kluczowe kryteria wyboru rozwiązań do uwierzytelniania i zarządzania dostępem

Zgodność z celem bezpieczeństwa Twojej organizacji	Szczegółowość autoryzacji i kontroli dostępu	Automatyzacja uwierzytelniania użytkowników i przydzielania dostępu
Możliwość monitorowania sesji uprzywilejowanych użytkowników	Tymczasowe przydzielanie dostępu	Elastyczność i możliwości integracyjne

Zapanuj nad hasłami swoich pracowników. Wdrożenie rozwiązań do zarządzania hasłami chroni Twoją organizację przed nieodpowiednimi nawykami związanymi z hasłami pracowników i przenosi odpowiedzialność za dostarczanie danych uwierzytelniających na personel bezpieczeństwa. Preferuj rozwiązania, które pozwalają na automatyzację rotacji haseł, szyfrowanie poświadczeń i dostarczanie jednorazowych haseł użytkownikom zewnętrznym.

Uzyskaj zgodność z NIS2 dzięki Ekran System

Ekran System to platforma do zarządzania pełnym cyklem ryzyka wewnętrznego, zaprojektowana w celu powstrzymywania, wykrywania i zapobiegania zagrożeniom wewnętrznym. Ekran System, wyposażony w bogaty zestaw narzędzi, może pomóc Twojej organizacji zwiększyć poziom cyberbezpieczeństwa i wdrożyć większość wymagań NIS2 za pomocą jednego rozwiązania.

Poniżej kilka sposobów, w jaki można wykorzystać Ekran System do zarządzania ryzykiem wewnętrznym i poprawy cyberbezpieczeństwa organizacji:

- **Monitoruj i rejestruj aktywność swoich pracowników i osób trzecich**, aby zobaczyć, w jaki sposób wchodzą w interakcję z wrażliwymi zasobami
- **Zarządzaj uprawnieniami dostępu i weryfikuj tożsamość użytkowników za pomocą 2FA**, aby zapobiec nieautoryzowanemu dostępowi do krytycznych punktów końcowych
- **Wdróż podejście just-in-time** i zabezpiecz wrażliwe dane, przyznając tymczasowy dostęp swoim partnerom, zewnętrznym firmom i dostawcom
- **Otrzymuj powiadomienia w czasie rzeczywistym o podejrzanych zachowaniach** użytkowników, aby Twój zespół ds. bezpieczeństwa mógł wyprzedzać zagrożenia
- **Skonfiguruj opcje automatycznego reagowania na incydenty**, aby szybko zamykać podejrzane procesy i blokować użytkowników naruszających zasady bezpieczeństwa
- **Wysyłaj ostrzeżenia do użytkowników**, którzy naruszają zasady bezpieczeństwa, aby przypomnieć im o korporacyjnych zasadach.
- **Generuj niestandardowe raporty**, aby uzyskać więcej szczegółów na temat aktywności pracowników i przeprowadzaj audyty bezpieczeństwa.

Lista ta może być zdecydowanie dłuższa. Aby zobaczyć, jak Ekran System może pomóc w spełnieniu wymagań cyberbezpieczeństwa NIS2 przeczytaj nasze szczegółowe zestawienie poniżej.

Mapowanie wymagań NIS2 na funkcjonalność Ekran System

Wymagane środki bezpieczeństwa	Odpowiadająca funkcjonalność Ekran System
Analiza ryzyka i bezpieczeństwo systemów informacyjnych	• Zarządzaj ryzykiem cyberbezpieczeństwa dzięki możliwościom zarządzania zagrożeniami wewnętrznymi Ekran System. • Zwiększ widoczność i wykrywaj ryzyko cyberbezpieczeństwa dzięki ciągłemu monitorowaniu aktywności użytkowników. • Egzekwuj polityki kontroli dostępu, zarządzaj dostępem użytkowników na poziomie szczegółowym i monitoruj aktywność uprzywilejowanych użytkowników.
Obsługa incydentów i raportowanie	• Zarządzaj zagrożeniami w czasie rzeczywistym, szybko identyfikując i reagując na incydenty bezpieczeństwa. • Przeglądaj szczegółowe nagrania sesji użytkowników, aby odtworzyć łańcuch zdarzeń. • Dostarczaj władzom kompleksowy dziennik audytu dzięki funkcjonalności audytu i raportowania Ekran System. • Eksportuj dowody cyberbezpieczeństwa do celów sądowych.
Ciągłość działania	• Szybko wykrywaj zdarzenia bezpieczeństwa, które mogą potencjalnie prowadzić do kryzysu, dzięki alertom w czasie rzeczywistym dotyczącym aktywności użytkowników. • Wykorzystaj nagrania sesji i dzienniki aktywności użytkowników do oceny wpływu na systemy i dane oraz do opracowywania planów i procedur odzyskiwania. • Zmniejsz ryzyko nieautoryzowanej aktywności, która może zakłócić działalność biznesową, przejmując kontrolę nad uprawnieniami dostępu w swojej infrastrukturze IT. • Ułatwiaj komunikację, dostarczając dokładne i szczegółowe informacje o kryzysie i jego skutkach. • Przywróć dziennik audytu swojej organizacji i kontynuuj monitorowanie i rejestrowanie aktywności użytkowników w przypadku awarii serwera dzięki trybom Wysokiej Dostępności i Disaster Recovery Ekran System.

Wymagane środki bezpieczeństwa	Odpowiadająca funkcjonalność Ekran System
Ocena skuteczności środków zarządzania ryzykiem w cyberbezpieczeństwie	• Wykorzystaj dziennik audytu generowany przez Ekran System do oceny, jak działają środki cyberbezpieczeństwa w Twojej organizacji. • Monitoruj, jak Twoi pracownicy i inni użytkownicy przestrzegają polityk bezpieczeństwa danych i innych zasad cyberbezpieczeństwa w Twojej organizacji.
Bezpieczeństwo łańcucha dostaw	• Monitoruj aktywność dostawców zewnętrznych, partnerów i innych podmiotów łańcucha dostaw, którzy mają dostęp do Twojej infrastruktury. • Weryfikuj i zarządzaj tożsamościami członków łańcucha dostaw, którzy mają dostęp do Twojej infrastruktury. • Zabezpiecz połączenia RDP do swojego środowiska i wykrywaj nieautoryzowany dostęp do danych, kradzież danych lub jakiekolwiek zachowanie zdalnego użytkownika wskazujące na potencjalne zagrożenie wewnętrzne. • Chroń dostęp do wrażliwych danych i kluczowych systemów, dostarczając dostawcom zewnętrznym jednorazowe hasła i ograniczając czas ich sesji w Twojej infrastrukturze IT. • Zwiększaj bezpieczeństwo swojego łańcucha dostaw, opcjonalnie instalując Ekran System na końcówkach dostawców zewnętrznych.
Podstawowe praktyki cyberhigieny i szkolenia w zakresie cyberbezpieczeństwa	• Uzyskaj widoczność działań i zachowań użytkowników, aby zidentyfikować i rozwiązać wszelkie braki w podstawowych praktykach higieny cybernetycznej i wykryć naruszenia polityki. • Monitoruj działania użytkowników podczas testów penetracyjnych, aby dostarczyć użytkownikom ukierunkowane informacje zwrotne i promować przestrzeganie najlepszych praktyk w zakresie cyberbezpieczeństwa. • Wykorzystaj nagrane sesje użytkowników do opracowywania materiałów i studiów przypadków dla inicjatyw szkoleniowych z zakresu świadomości cyberbezpieczeństwa. • Kształtuj nawyki cyberbezpieczeństwa użytkowników, wyświetlając komunikaty ostrzegawcze w odpowiedzi na zabronione działania.

Wymagane środki bezpieczeństwa	Odpowiadająca funkcjonalność Ekran System
Polityki i procedury dotyczące stosowania kryptografii i szyfrowania	• Wykorzystaj szyfrowanie danych monitorowania aktywności użytkowników, połączeń i innych wrażliwych rekordów Ekran System. • Zabezpiecz hasła i poświadczenia użytkowników Twojej organizacji za pomocą algorytmów SHA-256 i AES-256. • Szyfruj wyeksportowane dane sesji użytkowników za pomocą RSA-1024, aby zapobiec jakimkolwiek zmianom w dowodach sądowych. • Wykorzystaj certyfikowane szyfrowanie FIPS 140-2 wszystkich nazw użytkowników i aliasów za pomocą funkcji anonimizacji danych Ekran System.
Stosowanie uwierzytelniania wieloskładnikowego lub ciągłego	• Zmniejsz ryzyko nieautoryzowanego dostępu i kompromitacji konta za pomocą uwierzytelniania dwuskładnikowego. • Wykorzystaj możliwości zarządzania hasłami i tożsamością Ekran System do ustanowienia bezpiecznego procesu żądania i zatwierdzania dostępu oraz do zwiększenia procedur uwierzytelniania w Twojej organizacji. • Zintegruj Ekran System z Active Directory i systemami obsługi zgłoszeń (Help-Desk).
Bezpieczeństwo zasobów ludzkich, polityki kontroli dostępu i zarządzanie zasobami	• Zapewnij bezpieczeństwo zasobów ludzkich, wykrywając i badając wszelkie nieautoryzowane lub podejrzane działania prowadzone przez pracowników. • Kontroluj dostęp do wrażliwych zasobów i wdrażaj zasadę najmniejszych uprawnień za pomocą funkcji zarządzania uprzywilejowanym dostępem Ekran System. • Rejestruj interakcje użytkowników z kluczowymi zasobami i systemami, aby zapewnić śledzenie zasobów, odpowiedzialność i ochronę.

Case study

Osadkowski-Cebulski: Jak zapewnić transparentność we współpracy z firmami zewnętrznymi dzięki Ekran System?

Wyzwanie

Przedsiębiorstwo z uwagi na częste korzystanie z usług firm zewnętrznych poszukiwało oprogramowania dostosowanego do praktyki biznesowej, jaką jest outsourcing IT. Głównym powodem była potrzeba monitorowania aktywności podejmowanych przez firmy świadczące usługi zdalne, audytowanie wykonanej pracy oraz możliwość kontrolowania czasu wykonania wszelkich działań.

Potrzeby firmy:

- Monitorowanie aktywności pracowników zewnętrznych
- Audytowanie wykonywanej na serwerach pracy
- Kontrola czasu wykonywanych obowiązków

Wynik

Do najważniejszych korzyści należy przede wszystkim stałe rozwijanie działu IT firmy naszego klienta. Dzięki wykorzystaniu Ekran System, przedsiębiorstwo ma możliwość oceny jakości wykonywanej przez firmy zewnętrzne pracy oraz racjonalne inwestowanie w usługi oraz cyberstrategię.

Dzięki współpracy z inżynierami Securivy możliwa była indywidualna konfiguracja oprogramowania, co pozwoliło na dostosowanie wszelkich ustawień zgodnie z wolą klienta.

Rozwiązanie

Firma wybrała standardowy schemat wdrożenia z pojedynczym agentem na serwerze terminalowym Windows RDS. Środowisko opiera się na architekturze z użyciem serwera przesiadkowego. Takie rozwiązanie jest jedną z najlepszych praktyk bezpieczeństwa IT, ponieważ pozwala na monitorowanie wszystkich użytkowników, chcących zdalnie połączyć się z firmowymi serwerami. Wykorzystanie Jump Servera wymusza na użytkownikach zdalnych, aby logowanie do wybranego serwera odbywało się jedynie poprzez nadzorowany serwer przesiadkowy.

Firma wykorzystuje oprogramowanie przede wszystkim w celu monitorowania pracowników oraz bezproblemowego rozliczania wykonanych prac, za sprawą obszernych i rozbudowanych dzienników audytu. Ekran System regularnie pomaga przy analizie prac serwisowych wykonywanych przez firmy zewnętrzne.

Pan Dariusz Majda początkowo wziął udział w prezentacji przeprowadzonej przez jednego z naszych inżynierów. Przedstawiała ona pełną funkcjonalność programu. Spotkanie to okazało się początkiem długoletniej i bezproblemowej współpracy.

W przypadku programów służących do monitorowania aktywności użytkowników na urządzeniach, najszerszym, jeśli chodzi o zakres prac, jest zwykle etap wdrożenia i wstępnej konfiguracji. Wyjątkiem jest Ekran System, który w przeciwieństwie do innych produktów tego typu na rynku, jest prosty, szybki i intuicyjny we wdrożeniu.

> *Aktualnie Ekran System spełnia wszystkie nasze oczekiwania i sprawdza się doskonale w monitorowaniu i rozliczaniu prac pracowników własnych jak i firm zewnętrznych. [...]*
>
> *Dzięki takiemu rozwiązaniu możemy rozwijać dział IT, sprawnie rozliczać pracowników własnych jak i firm trzecich oraz panować nad rzetelnym rozliczaniem kosztów i planować dalsze inwestycje.*
>
> **Dariusz Majda**
> Specjalista IT w firmie Osadkowski-Cebulski

Czytaj dalej

...o sukcesie naszego klienta.

Case Study | Zapewnienie zgodności i zarządzanie ryzykiem wewnętrznym z Ekran System

Historia sukcesu klienta

Europejski dostawca usług zdrowotnych AGEL chroni wrażliwe dane przed zagrożeniami wewnętrznymi za pomocą Ekran System

Wyzwanie

AGEL to duży dostawca usług zdrowotnych, który pracuje z wrażliwymi danymi klientów, więc musi je chronić zgodnie z wymogami branżowymi. Aby utrzymać zgodność, AGEL potrzebował rozwiązania, które pozwoli:

- Ustanowić niezawodny nadzór nad danymi zdrowotnymi
- Audytować aktywność administratora
- Zarządzać dostępem uprzywilejowanych użytkowników
- Utrzymywać wygodną infrastrukturę Multi-tenant

Rozwiązanie

Oto, jak AGEL zabezpieczył dane medyczne i wdrożył wymogi branżowe za pomocą Ekran System:

- Ustanowiono monitorowanie aktywności użytkowników, aby śledzić aktywność administratora i zwiększyć widoczność interakcji użytkowników z wrażliwymi danymi
- Skonfigurowano alerty dotyczące aktywności użytkowników, aby identyfikować podejrzane działania i szybko reagować na zagrożenia
- Wykorzystano możliwości zarządzania uprzywilejowanym dostępem Ekran System, aby zapewnić administratorom bezpieczny dostęp do kluczowych serwerów
- Wykorzystano tryb multi-tenant, aby móc zarządzać Ekran System oddzielnie dla każdej placówki AGEL

Wynik

Nasz klient skutecznie zwiększył bezpieczeństwo wrażliwych danych bez zmian w procedurach zarządzania systemem. Wdrożyli Ekran System bezpośrednio na kluczowych punktach końcowych, co pozwoliło im:

- Zobaczyć, kto co robi z wrażliwymi danymi
- Reagować na zagrożenia wewnętrzne w czasie rzeczywistym
- Ograniczyć dostęp administratora do konkretnej placówki
- Zarządzać konfiguracjami serwerów oddzielnie dla każdej placówki
- Utrzymywać zgodność z przepisami branżowymi

> *Rozwiązanie Ekran System pomogło nam uzyskać pełną kontrolę nad działaniami uprzywilejowanych użytkowników pracowników zewnętrznych na wybranych serwerach i terminalach AGEL Group.*
>
> **Jan Pavlik**

Historia sukcesu klienta

Amerykańska firma świadcząca usługi finansowe skutecznie monitoruje i audytuje uprzywilejowanych użytkowników

Wyzwanie

Amerykańska organizacja finansowa szukała rozwiązania, które mogłoby:

- Monitorować aktywność użytkowników na serwerach przesiadkowych
- Zbierać dane o aktywności użytkowników do celów audytów zgodności
- Wspierać systemy operacyjne Windows i Linux
- Pozwalać na aktualizacje offline

Rozwiązanie

Aby sprostać swoim potrzebom w zakresie cyberbezpieczeństwa, klient wykorzystał możliwości Ekran System do następujących zadań:

- Ustanowiono solidne monitorowanie aktywności użytkowników, aby określić, jakie dane są dostępne, przez kogo i w jakim celu
- Wykorzystano przeszukiwalne nagrania sesji użytkowników do analizy aktywności użytkowników uprzywilejowanych
- Skonfigurowano generowanie niestandardowych raportów, aby przyspieszyć i uprościć zarówno audyty wewnętrzne, jak i zewnętrzne
- Zorganizowano monitorowanie kluczowych serwerów działających na systemach Windows i Linux
- Przeprowadzono ręczne aktualizacje platformy bez połączenia z Internetem (stand-alone), aby zapewnić maksymalną ochronę krytycznych danych

Wynik

Wdrożenie Ekran System pozwoliło naszemu klientowi sprostać każdemu z ich kluczowych wymagań i osiągnąć następujące wyniki:

- Uzyskać wgląd w aktywność użytkowników na serwerach terminali
- Zapewnić szybkie i efektywne audyty wewnętrzne
- Utrzymać zgodność z cyberbezpieczeństwem
- Wykrywać w czasie rzeczywistym i zatrzymywać złośliwą aktywność wewnętrzną

> *Ekran System był jedynym rozwiązaniem, które pozwoliło nam monitorować serwery działające na różnych systemach operacyjnych i instalować krytyczne aktualizacje offline. Otrzymanie tej samej funkcjonalności monitorowania za rozsądną cenę było nieoczekiwaną korzyścią z tej współpracy.*

Podsumowanie

NIS2 wymaga od podmiotów krytycznych wdrożenia szerokiego zakresu wymogów, określonych w art. 21 dyrektywy. Rozsądnie jest rozpocząć przygotowania już teraz, ponieważ każde państwo członkowskie UE musi dostosować wymogi NIS2 do prawa krajowego do października 2024 roku. Jeśli Twoja organizacja jest kluczowym lub ważnym podmiotem, zgodnie z definicją zawartą w dyrektywie, musisz wypełnić wszelkie luki między obecnym stanem cyberbezpieczeństwa a wymogami.

W zależności od obecnego poziomu zgodności, możesz potrzebować pomocy technicznej i rozwiązań, aby spełnić określone wymagania NIS2. Rozwiązaniem może być Ekran System. Jako kompleksowa platforma do zarządzania ryzykiem wewnętrznym, Ekran System oferuje wiele możliwości cyberbezpieczeństwa w ramach jednej platformy, pomagając zwiększyć następujące obszary bezpieczeństwa opisane przez NIS2:

- ✓ Analiza ryzyka i bezpieczeństwo systemów informatycznych
- ✓ Obsługa i raportowanie incydentów
- ✓ Ciągłość działania
- ✓ Bezpieczeństwo łańcucha dostaw
- ✓ Ocena środków zarządzania ryzykiem cyberbezpieczeństwa
- ✓ Podstawowe praktyki higieny cybernetycznej i szkolenia
- ✓ Kryptografia i szyfrowanie
- ✓ Bezpieczeństwo zasobów ludzkich, zasady kontroli dostępu i zarządzanie zasobami
- ✓ Uwierzytelnianie wieloskładnikowe

Skontaktuj się z nami, aby omówić możliwości Ekran System w zakresie zgodności z regulacjami i przetestuj produkt w ramach bezpłatnego 30-dniowego okresu próbnego. Możesz również otrzymać bezpłatny dostęp do portalu demonstracyjnego online, abyś mógł sprawdzić wszystkie funkcje Ekran System.

Spełnij wymagania NIS2 i zwiększ poziom cyberbezpieczeństwa dzięki Ekran System

Odwiedź stronę www.ekransystem.com/pl i securivy.com lub napisz do nas na adres biuro@securivy.com

Ekran

Z czym wiąże się uzyskanie zgodności z NIS2?

Aby uzyskać zgodność z najnowszą Dyrektywą NIS2, należy nie tylko przejść szereg kroków profesjonalnie przygotowanej ścieżki implementacji rozwiązań. Warto zacząć od analizy dotychczasowych zabezpieczeń, narzędzi i systemów zarządzania ryzykiem ICT w swojej firmie. Czy przeprowadzasz wewnętrzne audyty bezpieczeństwa oraz szkolenia pracowników? Czy obowiązki w przypadku reagowania na incydenty bezpieczeństwa są odpowiednio rozdzielone? **Niezależnie od odpowiedzi, każda firma potrzebuje kompleksowego rozeznania, na które składają się:**

1. DIAGNOZA

Analiza profilu działalności firmy, określenie zakresu objęcia regulacją i przedziału przepisów mających zastosowanie do organizacji.

2. AUDYT

Ocena przygotowania przedsiębiorstwa do spełnienia wymogów NIS2 - identyfikacja kluczowych obszarów i luk wymagających uzupełnienia.

3. ANALIZA RYZYKA

Określenie potencjalnych zagrożeń dla organizacji w kontekście dyrektywy - identyfikacja dzięki narzędziom do szacowania ryzyka.

4. PLAN DZIAŁAŃ

Przygotowanie planu działań i zmian, który pozwoli na egzekwowanie kolejnych kroków w ustalonym przedziale czasowym.

5. RAPORT

Sporządzenie dokumentu zawierającego rekomendacje i zakresy wymaganych zmian, a także zdefiniowany budżet potrzebny na realizację.

6. IMPLEMENTACJA

Weryfikacja, przygotowanie, a także przejście przez implementację według wcześniej ustalonych punktów.

Jak wygląda wdrożenie Ekran System z nami?

- **20-minutowa konsultacja**
  Podczas tej rozmowy nasz Product Manager przeprowadzi z Tobą wstępne rozeznanie w kwestii potrzeb firmy oraz ocenimy zakres działań.
- **Analiza przypadku**
  Przeprowadzimy z Tobą wstępne rozeznanie w kwestii potrzeb firmy oraz ocenimy zakres potrzebnych działań.
- **Propozycja oferty, rozwiązania oraz szkolenie**
  Na tym etapie otrzymujesz od nas szczegółową informację dotyczącą rozwiązania, a także budżetu potrzebnego na implementację. Przeprowadzamy też krótkie szkolenie dotyczące wdrożenia.
- **Przygotowanie klienta**
  Samodzielnie przechodzisz przez wytyczone szczegółowo na naszej checkliście kroki, które pozwolą na przygotowanie infrastruktury pod instalację.
- **Wdrożenie rozwiązania**
  Konfiguracja narzędzia Ekran System przez nasz zespół.

ROZPOCZNIJ KONSULTACJE JUŻ TERAZ

Grzegorz Fijałkowski
Product Manager

Jako Twój opiekun w sprawie wdrożenia rozwiązań dla zgodności NIS2 zadbam, by każdy etap przebiegał sprawnie i płynnie.

Skontaktuj się ze mną
grzegorz.fijalkowski@securivy.com
+48 724 804 952
lub napisz
bezpośrednio w Microsoft Teams