Syteca
formerly Ekran System

SECURIVY

EBOOK

Poradnik Osiągnięcia i Utrzymania Zgodności z DORA

10 kroków do zbudowania cyfrowej odporności operacyjnej

- Uzyskaj zgodność z wymaganiami DORA
- Popraw swoje cyberbezpieczeństwo
- Przyspiesz wykrywanie incydentów
- Usprawnij proces raportowania zdarzeń
- Zarządzaj zagrożeniami stron trzecich
- Zwalczaj zagrożenia wewnętrzne

www.syteca.com www.securivy.com

biuro@securivy.com

Wstęp

Podczas gdy budżety na cyberbezpieczeństwo wcale nie rosną, cyberzagrożenia stają się coraz częstsze i bardziej dopracowane. Instytucje finansowe są więc dziś narażone na ataki jak nigdy dotąd.

Aby pomóc instytucjom finansowym działającym w Europie w zwalczaniu ataków cybernetycznych i utrzymaniu procesów biznesowych podczas incydentów bezpieczeństwa, Komisja Europejska wprowadziła ustawę o cyfrowej odporności operacyjnej.

> W erze cyfrowej, technologie informacyjno-komunikacyjne (ICT) wspierają złożone systemy wykorzystywane w codziennych czynnościach. Utrzymują one naszą gospodarkę w ruchu w kluczowych sektorach, w tym w sektorze finansowym, oraz zwiększają funkcjonowanie wewnętrznego rynku. Wzmożona digitalizacja i wzajemna łączność również zwiększają ryzyko związane z ICT, co czyni całe społeczeństwo, a w szczególności system finansowy, bardziej podatnym na zagrożenia cybernetyczne lub zakłócenia ICT.
>
> Chociaż wszechobecne wykorzystanie systemów ICT oraz wysoka digitalizacja i łączność są dziś kluczowymi cechami działalności unijnych podmiotów finansowych, ich odporność cyfrowa wciąż wymaga lepszego uwzględnienia i zintegrowania z szerszymi ramami operacyjnymi.
>
> **Ustawa o cyfrowej odporności operacyjnej, Preambuła 1**

Celem niniejszego poradnika jest zapewnienie podmiotom finansowym kompleksowego zrozumienia ustawy o cyfrowej odporności operacyjnej. Whitepaper składa się z dziesięciu praktycznych kroków w celu spełnienia wymogów ustawy i pokazuje, w jaki sposób Syteca by Ekran System może pomóc na drodze tego procesu.

Spis treści

Wszystko co musisz wiedzieć o Rozporządzeniu DORA 4

Czym jest DORA? 4

Czym jest odporność operacyjna? 4

Czy wymogi DORA dotyczą Twojej organizacji? 5

Pięć filarów Rozporządzenia DORA 7

Jakie korzyści płyną ze zgodności z DORA? 8

Konsekwencje nieuzyskania zgodności 8

Kroki do uzyskania zgodności 9

Krok 1. Stworzenie ram zarządzania ryzykiem ICT 9

Krok 2. Opracowanie strategii cyfrowej odporności cyfrowej 10

Krok 3. Wdrożenie narzędzi, polityk i procedur bezpieczeństwa ICT 11

Krok 4. Wdrożenie rozwiązań do wykrywania incydentów 12

Krok 5. Stworzenie planu ciągłości działania ICT 13

Krok 6. Opracowanie procedur tworzenia kopii i odzyskiwania danych 14

Krok 7. Utrzymanie świadomości w zakresie cyberbezpieczeństwa 15

Krok 8. Tworzenie procesu zarządzania incydentami 16

Krok 9. Przeprowadzanie cyfrowych testów odporności operacyjnej 18

Krok 10. Zarządzanie ryzykiem zewnętrznym 19

Zgodność z DORA dzięki rozwiązaniu Syteca 21

Wspieranie pięciu filarów DORA za pomocą Syteca 22

Case studies | Zapewnienie zgodności i zarządzanie ryzykiem wewnętrznym za pomocą Syteca 24

Podsumowanie 27

Wszystko co musisz wiedzieć o Rozporządzeniu DORA

Przed przystąpieniem do konkretnych działań, kluczowe znaczenie ma dokładne przestudiowanie pełnej treści rozporządzenia. W tej sekcji zagłębiamy się w podstawowe informacje na temat ustawy o cyfrowej odporności operacyjnej. Pokrótce omówimy najważniejsze informacje dotyczące tego rozporządzenia, aby pomóc Ci zrozumieć, na czym należy się skupić i jak się przygotować.

Czym jest DORA?

Rozporządzenie o cyfrowej odporności operacyjnej (DORA) to ustawa, która określa wymogi dla podmiotów finansowych:

- Ograniczanie ryzyka związanego z technologiami informacyjno-komunikacyjnymi (ICT)
- Zapewnienie odpowiedniej ochrony, wykrywania, powstrzymywania i odzyskiwania danych w przypadku incydentów związanych z ICT

Znana również jako Regulacja (EU) 2022/2554, DORA weszła w życie w Unii Europejskiej 17 stycznia 2023 roku. Jej głównym celem jest zwiększenie odporności operacyjnej organizacji finansowych w Unii Europejskiej.

Czym jest odporność operacyjna?

> Odporność operacyjna to zdolność podmiotu finansowego do budowania, zapewniania i przeglądania swojej integralności operacyjnej oraz niezawodności poprzez uzyskanie, bezpośrednio lub pośrednio za pomocą usług świadczonych przez zewnętrznych dostawców usług ICT, pełnego zakresu możliwości związanych z ICT, niezbędnych do utrzymania bezpieczeństwa sieci i systemów informacyjnych wykorzystywanych przez podmiot finansowy, które wspierają ciągłość świadczenia usług finansowych oraz ich jakość, w tym podczas zakłóceń.
>
> **Ustawa o cyfrowej odporności operacyjnej, Artykuł 3**

DORA sugeruje, że zamiast koncentrować wysiłki na zapobieganiu, reagowaniu i eliminowaniu zakłóceń w działalności, organizacje finansowe muszą rozwijać zdolność do dalszego dostarczania świadczenia podstawowych usług nawet w obliczu takich problemów. Temu celowi służy właśnie odporność operacyjna.

Czy DORA ma zastosowanie przy Twojej organizacji?

Przed rozpoczęciem działań mających na celu osiągnięcie zgodności z przepisami DORA należy upewnić się, że regulacja ma zastosowanie do Twojej organizacji.

Zakres DORA obejmuje różne podmioty finansowe działające w UE takie jak:

- Instytucje kredytowe
- Instytucje płatnicze, w tym wyłączone na mocy regulacji (UE) 2015/2366
- Dostawcy usług informacji o kontach
- Instytucje płatności elektronicznych, w tym wyłączone zgodnie z regulacją 2009/110/WE
- Firmy inwestycyjne
- Dostawcy usług związanych z kryptoaktywami zgodnie z Rozporządzeniem Parlamentu Europejskiego i Rady w sprawie rynków kryptoaktywów oraz zmianami rozporządzeń: (UE) nr 1093/2010, (UE) nr 1095/2010, regulacji 2013/36/UE, (UE) 2019/1937 („rozporządzenie w sprawie rynków kryptoaktywów"), a także emitenci tokenów powiązanych z aktywami
- Centralne depozyty papierów wartościowych
- Kontrahenci centralni
- Systemy transakcyjne
- Repozytoria handlowe
- Zarządzający alternatywnymi funduszami inwestycyjnymi
- Spółki zarządzające
- Dostawcy usług raportowania danych
- Zakłady ubezpieczeń i reasekuracji
- Pośrednicy ubezpieczeniowi, reasekuracyjni pośrednicy ubezpieczeniowi, pośrednicy reasekuracyjni pośrednicy ubezpieczeniowi
- Instytucje pracowniczych planów emerytalnych
- Agencje ratingowe
- Administratorzy krytycznych wskaźników
- Dostawcy usług finansowania społecznościowego
- Repozytoria papierów wartościowych
- Zewnętrzni dostawcy usług ICT

Istnieje jednak kilka wyjątków. Poniżej znajdują się organizacje finansowe zwolnione z obowiązku uzyskania zgodności z DORA:

- ✗ Zarządzający alternatywnymi funduszami inwestycyjnymi zgodnie z art. 3 ust. 2 regulacji 2011/61/UE
- ✗ Zakłady ubezpieczeń i zakłady reasekuracji zgodnie z art. 4 regulacji 2009/138/WE
- ✗ Instytucje pracowniczych programów emerytalnych obsługujące programy emerytalne, które łącznie nie mają więcej niż 15 członków
- ✗ Osoby fizyczne lub prawne zwolnione zgodnie z art. 2 i 3 regulacji 2014/65/UE
- ✗ Pośrednicy ubezpieczeniowi, pośrednicy reasekuracyjni i pomocniczy pośrednicy ubezpieczeniowi którzy są mikroprzedsiębiorstwami albo małymi lub średnimi przedsiębiorstwami
- ✗ Instytucje świadczące żyro pocztowe, o których mowa w art. 2 ust. 5 pkt 3 regulacji 2013/36/UE

Jeśli Twoja organizacja należy do tych, które są zobowiązane do przestrzegania DORA, masz czas do 17 stycznia 2025 r., aby spełnić jej wymogi.

Pięć filarów DORA

Aby osiągnąć zgodność, organizacje finansowe muszą skoncentrować swoje wysiłki na pięciu podstawowych filarach DORA. Te kluczowe obszary stanowią podstawę wymagań DORA, kierując organizacje we wzmacnianiu ich odporności operacyjnej.

01

Zarządzanie Ryzykiem ICT

ROZDZIAŁ II (artykuły 5-16) określa procedury i polityki bezpieczeństwa, które instytucje finansowe muszą ustanowić i regularnie aktualizować, aby umożliwić właściwy proces zarządzania ryzykiem ICT.

02

Zarządzanie Incydentami Związanymi z ICT

ROZDZIAŁ III (artykuły 17-23) stwierdza, że odpowiednie podmioty muszą posiadać środki umożliwiające szybkie wykrywanie, klasyfikowanie i zgłaszanie incydentów związanych z ICT, a także ustanawiać odpowiedzialności i plany łagodzenia skutków dla różnych scenariuszy incydentów.

03

Testowanie Odporności Operacyjnej w Zakresie ICT

ROZDZIAŁ IV (artykuły 24-27) doradza organizacjom finansowym ocenę i testowanie ich gotowości na obsługę incydentów związanych z ICT przynajmniej raz w roku, w celu identyfikacji i eliminowania luk w odporności operacyjnej.

04

Zarządzanie Ryzykiem Związanym z Zewnętrznymi Usługami ICT

ROZDZIAŁ V (artykuły 28-44) określa zasady i wymagania, których muszą przestrzegać podmioty finansowe, aby zapewnić bezpieczną współpracę z dostawcami usług ICT i właściwie zarządzać ryzykami związanymi z zewnętrznymi podmiotami.

05

Wymiana Informacji

ROZDZIAŁ VI (artykuł 45) zachęca instytucje finansowe do wymiany informacji o zagrożeniach cybernetycznych i danych wywiadowczych w celu wzmocnienia odporności cyfrowej w całym sektorze.

Jakie korzyści niesie za sobą DORA?

Zapewnienie zgodności z przepisami DORA może wydawać się czasochłonne i przytłaczające, jeśli okaże się, że trzeba zmienić ustalone procesy i wprowadzić nowe zasady i procedury. Ostatecznie jednak spełnienie tych wymagań dotyczących bezpieczeństwa będzie korzystne dla Twojej firmy, ponieważ uzyskasz następujące korzyści:

Podwyższone bezpieczeństwo firmy

Ochrona wrażliwych danych

Minimalizacja zagrożeń cybernetycznych

Szybkie wykrywanie podejrzanych akcji

Efektywne zarządzanie incydentami

Wymiana doświadczeń w zakresie ograniczania ryzyka związanego z ICT

Konsekwencje nieuzyskania zgodności

Naruszenie wymogów DORA może prowadzić do nałożenia kar administracyjnych. Grzywny te mogą wynosić nawet 1% średnich dziennych globalnych zarobków organizacji z poprzedniego roku podatkowego. Organizacje niespełniające wymogów mogą nawet ponieść dalsze konsekwencje, takie jak:

- **Koszty działań naprawczych** niezbędnych do wyeliminowania luk w zabezpieczeniach lub awarii odporności operacyjnej organizacji.
- **Publiczne nagany** dotyczące nieprzestrzegania przez organizację wymogów DORA.
- **Płatności odszkodowań** na rzecz klientów i stron trzecich dotkniętych skutkami związanymi z niezgodnością organizacji.
- **Cofnięcie autoryzacji** w przypadku powtarzającego się naruszenia wymogów DORA.

Kroki do uzyskania zgodności z DORA

Rozpoczęcie działań mających na celu uzyskanie zgodności z DORA może być wymagające. Aby ułatwić to zadanie, proponujemy dziesięcioetapowy plan, który pomoże stopniowo spełnić wymagania DORA.

Krok 1. Stwórz ramy zarządzania ryzykiem ICT

Ustanowienie solidnych i kompleksowych ram zarządzania ryzykiem teleinformatycznym w ramach systemu zarządzania ryzykiem. Ramy te powinny umożliwić organizacji szybkie i skuteczne radzenie sobie z zagrożeniami teleinformatycznymi oraz określać elementy niezbędne do ochrony zasobów informacyjnych i teleinformatycznych.

> „Zasób informacyjny" oznacza zbiór informacji, materialnych lub niematerialnych, które są warte ochrony.
>
> „Zasób ICT" oznacza zasób programowy lub sprzętowy w sieci i systemach informacyjnych wykorzystywanych przez podmiot finansowy.
>
> **Ustawa o cyfrowej odporności operacyjnej, Artykuł 3**

Upewnij się, że Twoje ramy zarządzania ryzykiem ICT obejmują strategie, polityki, procedury, protokoły ICT i narzędzia wymagane do skutecznej ochrony wszystkich informacji i zasobów ICT organizacji. Aby zapewnić aktualność ram, zaleca się ich aktualizację co najmniej raz w roku.

Aby wesprzeć ramy, należy rozważyć stworzenie systemu zarządzania bezpieczeństwem informacji (ISMS). Zapewnia to ustrukturyzowane i systematyczne podejście do zarządzania bezpieczeństwem informacji w celu dalszego zmniejszenia ryzyka cyfrowego. Podczas tworzenia ISMS należy odnieść się do międzynarodowej normy ISO 27001, która określa wymagania, jakie powinien spełniać ISMS.

Niektóre organizacje finansowe kwalifikują się do uproszczonych ram zarządzania ryzykiem, które są łatwiejsze do wdrożenia. Więcej informacji na temat kwalifikujących się organizacji i uproszczonych wymogów ramowych można znaleźć w art. 16 DORA.

Krok 2. Opracowanie strategii cyfrowej odporności operacyjnej

Ramy zarządzania ryzykiem ICT z poprzedniego kroku zapewnią całościowy obraz środków ochrony zasobów organizacji. Po ich opracowaniu należy rozpocząć pracę nad strategią cyfrowej odporności operacyjnej, która pokaże, jak wykorzystać te środki w praktyce. Taka strategia musi określać elementy takie jak:

- **Dopasowanie między ramami a biznesem**
- **Tolerancja ryzyka organizacji**
- **Cele bezpieczeństwa informacji**
- **Plan architektury ICT**
- **Mechanizmy ochrony i wykrywania**
- **Aktualny stan cyfrowej odporności operacyjnej**
- **Implementacja testowania odporności operacyjnej ICT**
- **Strategia komunikacyjna**

Tworząc strategię cyfrowej odporności operacyjnej, należy określić, w jaki sposób ramy zarządzania ryzykiem ICT wspierają strategię biznesową i cele organizacji. Konieczne może być zidentyfikowanie kluczowych procesów i usług organizacji oraz określenie, w jaki sposób ustanowione ramy zarządzania ryzykiem ICT pomagają utrzymać je w nienaruszonym stanie.

Przeprowadź ocenę ryzyka ICT, aby określić jego poziom, który organizacja może tolerować, biorąc pod uwagę podatność organizacji i potencjalny wpływ zakłóceń ICT. Jasno zdefiniuj kluczowe wskaźniki wydajności (KPI) i kluczowe wskaźniki ryzyka, aby zmierzyć powodzenie inicjatyw związanych z bezpieczeństwem informacji.

Podaj architekturę ICT, której używasz jako odniesienia i określ zmiany potrzebne do zbudowania takiej architektury w Twojej organizacji i osiągnięcia celów biznesowych. Określ sposób, w jaki chronisz organizację przed incydentami związanymi z ICT, wykrywasz je i zmniejszasz ich wpływ.

Oceń swoją obecną cyfrową odporność operacyjną i udokumentuj jej aktualny stan w oparciu o liczbę poważnych incydentów związanych z ICT, których doświadczyła Twoja organizacja oraz skuteczność środków zapobiegawczych. Należy również określić sposoby testowania cyfrowej odporności operacyjnej organizacji.

Na koniec należy określić, w jaki sposób pracownicy i interesariusze powinni komunikować się podczas incydentów związanych z ICT.

Krok 3. Wdróż narzędzia, polityki i procedury bezpieczeństwa ICT

Aby wdrożyć strategię odporności cyfrowej, należy zastosować różne rozwiązania technologiczne oraz przyjąć nowe zasady i procedury bezpieczeństwa. W połączeniu powinny one służyć następującym celom:

Lista zasad, które należy opracować i wdrożyć w swojej organizacji finansowej, obejmuje:

- **Politykę bezpieczeństwa informacji** definiującą zasady i narzędzia wykorzystywane do ochrony danych organizacji i jej klientów.
- **Politykę kontroli dostępu** dotyczącą sposobu ograniczania dostępu do zasobów informacyjnych i zasobów ICT oraz zapewnienia, że dostęp jest udzielany wyłącznie z uzasadnionych powodów.
- **Zasady uwierzytelniania użytkowników** opisujące proces weryfikacji, czy osoba próbująca uzyskać dostęp do zasobów organizacji jest tym, za kogo się podaje.
- **Politykę szyfrowania** określającą metody szyfrowania danych i środki ochrony kluczy kryptograficznych.
- **Politykę zarządzania zmianami ICT** obejmującą sposób wdrażania i weryfikacji wszelkich zmian w systemach lub parametrach bezpieczeństwa.
- **Politykę zarządzania poprawkami** definiującą sposób i czas stosowania poprawek i aktualizacji w różnych systemach.

Oprócz tych zasad niezbędne jest opracowanie struktury zarządzania infrastrukturą, która uwzględnia potencjalne zagrożenia. Korzystanie z dedykowanych narzędzi i mechanizmów może szybko odizolować i zabezpieczyć krytyczne dane w przypadku cyberataku.

Step 4. Wprowadź rozwiązania do wykrywania incydentów

Zgodnie z art. 10 DORA, organizacje finansowe powinny posiadać możliwości monitorowania aktywności, które pozwolą im szybko zauważyć podejrzaną aktywność oznaczającą problemy z wydajnością sieci ICT i incydenty związane z ICT.

Wdrożenie rozwiązań do monitorowania aktywności użytkowników (UAM), wykrywania i reagowania w punktach końcowych (EDR), rozszerzonego wykrywania i reagowania (XDR) oraz zarządzania informacjami i zdarzeniami bezpieczeństwa (SIEM) może pomóc w uzyskaniu wglądu w to, co dzieje się w sieci. Aby w pełni wykorzystać proces monitorowania, należy postępować zgodnie z poniższymi najlepszymi praktykami:

1. Ciągłe monitorowanie aktywności użytkowników. Monitorowanie aktywności użytkowników nigdy nie powinno być traktowane jako jednorazowe wydarzenie. Jeśli jest wykonywane tylko okresowo, nie zapewni pełnego wglądu w działania użytkowników ani właściwej ochrony krytycznych danych.

2. Kontrola użycia urządzeń USB. Złośliwy insider może użyć dysku USB jako narzędzia do wycieku i naruszenia poufnych danych, kradzieży własności intelektualnej firmy lub przeprowadzenia wcześniej zaprogramowanej strategii ataku. Dlatego tak ważne jest, aby uważnie obserwować wszystkie połączenia USB.

3. Zarządzanie zdalnymi połączeniami. Im więcej użytkowników uzyskuje zdalny dostęp do danych i systemów organizacji, tym więcej może pojawić się obaw związanych z bezpieczeństwem. Z tego powodu warto rozważyć wdrożenie oprogramowania do monitorowania pulpitu zdalnego, aby wszystkie połączenia zdalne były ściśle monitorowane.

4. Analiza zachowań użytkowników. Zachowanie legalnego użytkownika znacznie różni się od zachowania zewnętrznego atakującego lub złośliwego insidera. Warto rozważyć wykorzystanie analizy zachowań użytkowników i podmiotów (UEBA) do szybkiego wykrywania nietypowych zachowań użytkowników sieci.

5. Automatyzacja odpowiedzi na incydenty. Przyspiesz reagowanie na incydenty związane z ICT dzięki rozwiązaniom technologicznym, które pozwalają skonfigurować automatyczne reakcje na incydenty w celu blokowania użytkowników i zatrzymywania podejrzanych procesów natychmiast po tym, jak odstąpią one od wcześniej zdefiniowanej reguły.

Krok 5. Stwórz plan ciągłości biznesu ICT

Należy opracować plan ciągłości działania ICT, który zawiera wytyczne, jakich organizacja musi przestrzegać w przypadku incydentu związanego z ICT. Pozwoli to na:

- **Zapewnienie ciągłości krytycznych operacji biznesowych**
- **Reagowanie na incydenty związane z ICT i ich rozwiązywanie**
- **Ograniczanie incydentów i zapobieganie dalszym stratom**
- **Szacowanie wstępnych strat i szkód**
- **Skuteczne raportowanie o incydentach odpowiednim władzom**

Aby stworzyć plan ciągłości działania ICT, sugerujemy przestrzeganie poniższych najlepszych praktyk:

1. Ocena i priorytetyzacja procesów biznesowych. Zacznij od zrozumienia procesów, które są najważniejsze dla Twojej firmy. Określ, które z nich są najbardziej krytyczne i najbardziej wrażliwe, a także jakie będą potencjalne straty, jeśli cokolwiek je zakłóci. Ocena i priorytetyzacja procesów biznesowych pomoże Ci zidentyfikować te, które są kluczowe dla Twojej firmy i muszą pozostać operacyjne przez cały czas trwania zakłóceń.

2. Zidentyfikuj RTO i RPO swojej organizacji. Cel czasu odzyskiwania (RTO) to pożądany czas między zatrzymaniem operacji biznesowych a ich przywróceniem, podczas gdy cel punktu odzyskiwania (RPO) odnosi się do maksymalnej utraty danych, jaką organizacja może tolerować. Kierownictwo organizacji musi zaangażować się w dyskusje, aby określić te cele w oparciu o charakter działalności, branżę, wymogi regulacyjne i inne szczegóły.

3. Określenie kroków i obowiązków. Biorąc pod uwagę wyniki oceny procesów biznesowych i cele odzyskiwania, określ, co należy zrobić i z kim się skontaktować podczas zakłóceń i przypisz osoby odpowiedzialne. Stwórz unikalny plan dla każdego z najbardziej prawdopodobnych incydentów związanych z ICT, aby nie były one zaskoczeniem.

Krok 6. Opracuj procedury tworzenia kopii zapasowych, przywracania i odzyskiwania danych

DORA ma na celu pomóc organizacjom finansowym zminimalizować zakłócenia i przestoje oraz wymaga, aby wszystkie z nich planowały procesy tworzenia kopii zapasowych, przywracania i odzyskiwania danych.

Opracuj i udokumentuj zasady tworzenia kopii zapasowych określających, jakie dane wymagają tworzenia kopii zapasowych i jak często, w oparciu o ważność i poufność. Określ także zasady i procedury przywracania oraz odzyskiwania danych, które określają, jakich lokalizacji odzyskiwania używasz do przechowywania kopii zapasowych i jak często replikujesz dane między nimi.

Pamiętaj, że musisz przechowywać kopie zapasowe w różnych lokalizacjach odzyskiwania, które są logicznie i fizycznie oddzielone od systemów organizacji, aby można je było odzyskać i uodpornić na różnego rodzaju zagrożenia.

Upewnij się, że aktywacja systemu kopii zapasowych nie wpływa na dostępność, autentyczność, integralność lub poufność danych. Zaimplementuj proces, który pozwoli na płynne działanie krytycznych usług podczas przywracania kopii zapasowej. W tym celu może być konieczne użycie redundantnych pojemności ICT, co oznacza ich duplikowanie na wypadek awarii oryginalnego systemu. W szczególności centralne depozyty papierów wartościowych powinny mieć dodatkowe miejsce przetwarzania:

1. Lokalizacja w geograficznej odległości od głównego miejsca przetwarzania

2. Możliwość utrzymania ciągłości funkcji krytycznych w sposób identyczny z lokalizacją podstawową

3. Dostępne dla pracowników w celu zapewnienia ciągłości krytycznych funkcji, gdy główne miejsce przetwarzania jest niedostępne

Gdy posiadasz już system kopii zapasowych, przetestuj go. Tak jak systemy biznesowe mogą zawieść podczas incydentu, to samo może się stać z kopiami zapasowymi. Mogą wystąpić problemy z konfiguracją, błędy oprogramowania lub awarie sprzętu, których nie rozpoznasz, jeśli nie przeprowadzisz testów.

Krok 7. Utrzymaj świadomość cyberbezpieczeństwa

Szkolenie uświadamiające ma zasadnicze znaczenie dla zapewnienia cyfrowej odporności operacyjnej organizacji finansowej. Nie można przecenić znaczenia świadomości w zakresie cyberbezpieczeństwa, ponieważ ryzyko wewnętrzne jest co najmniej tak samo istotne, jak ryzyko cyberataków.

Bez fundamentalnego zrozumienia podstawowej higieny cybernetycznej wśród liderów i pracowników organizacji, cyberbezpieczeństwo prawdopodobnie pozostanie zdezorganizowane. Poniżej przedstawiamy najlepsze praktyki w zakresie prowadzenia szkoleń podnoszących świadomość w zakresie cyberbezpieczeństwa:

1. Zdefiniuj odbiorców i zakres programu szkoleniowego

Zgodnie z wymogami DORA obowiązkowe jest prowadzenie szkoleń dla kadry kierowniczej i pracowników. Można jednak dostosować szkolenie do unikalnych potrzeb różnych grup w organizacji. Na przykład zapewnić zwykłym użytkownikom ogólną wiedzę na temat cyberbezpieczeństwa, jednocześnie prowadząc dogłębny kurs dla administratorów systemów i specjalistów ds. bezpieczeństwa oraz szkolenie w centrum biznesowym dla kadry kierowniczej.

2. Spraw, aby szkolenie było angażujące i istotne

Jeśli szkolenie jest nudne dla uczestników lub nie ma nic wspólnego z ich codzienną rutyną, nic z niego nie wyniosą. Aby sprawić, że kurs będzie wciągający, postaraj się:

- Unikać korzystania z generycznych materiałów szkoleniowych
- Łączyć różne rodzaje treści: wykłady, artykuły, filmy, quizy itp.
- Wyjaśnić, w jaki sposób niezgodność z zasadami cyberbezpieczeństwa wpływa na uczestników i całą firmę
- Przygotować przykłady incydentów związanych z bezpieczeństwem i ich konsekwencji

3. Symulacja incydentu związanego z ICT

Współpracuj z działem IT, aby przeprowadzić jeden lub kilka symulowanych ataków: wyślij wiadomość phishingową lub spróbuj użyć inżynierii społecznej, aby uzyskać poufne dane od pracowników itp. Następnie zbierz wyniki i przeanalizuj błędy popełnione przez pracowników oraz przyczyny tych błędów.

Aby uzyskać jak najlepsze wyniki, należy uzupełnić program szkoleniowy o najbardziej aktualne informacje na temat cyberzagrożeń. Przeanalizuj niektóre niedawne incydenty związane z technologiami informacyjno-komunikacyjnymi opublikowane przez europejskie organy nadzoru oraz informacje udostępnione przez inne instytucje finansowe.

Krok 8. Zbuduj proces zarządzania incydentami

Twoja organizacja finansowa powinna mieć proces zarządzania incydentami (IRP) - zestaw pisemnych instrukcji umożliwiających szybką reakcję na incydenty związane z ICT. IRP opracowuje środki mające na celu wykrycie i identyfikację incydentu, reagowanie na niego, łagodzenie jego skutków i zapewnienie, że nie wystąpi on ponownie.

Podczas opracowywania planu IRP należy przestrzegać wytycznych dotyczących planu reagowania na incydenty w oparciu o przewodnik NIST dotyczący obsługi incydentów związanych z bezpieczeństwem komputerowym.

Upewnij się, że Twój IRP ma jasno zdefiniowane następujące elementy:

- **Wczesne wskaźniki incydentów związanych z ICT**
- **Procedury identyfikacji, śledzenia, rejestrowania i klasyfikowania incydentów**
- **Role i odpowiedzialności dla różnych scenariuszy incydentów**
- **Plany komunikowania incydentu**
- **Procedury zgłaszania incydentów**
- **Działania naprawcze mające na celu złagodzenie skutków incydentu**

Wczesne wskaźniki incydentów związanych z ICT

Skompiluj listę działań, które mogą oznaczać potencjalny incydent związany z ICT i aktywnie obserwuj je podczas monitorowania aktywności użytkowników. Mogą istnieć różne wskaźniki incydentów bezpieczeństwa, takie jak:

- Odchylenie od typowego ruchu sieciowego
- Pracownik logujący się do systemu o nietypowych porach
- Wielokrotne nieudane próby logowania z nieznanego systemu zdalnego

Możesz wykorzystać rozwiązania technologiczne, które ostrzegą Cię za każdym razem, gdy w Twojej infrastrukturze pojawi się wskaźnik, a nawet automatycznie reagować na podejrzaną aktywność.

Procedury identyfikacji, śledzenia, rejestrowania i klasyfikowania incydentów

Utwórz i udokumentuj procedury reagowania na incydenty związane z ICT na wszystkich etapach, od przygotowania po działania po incydencie. Określ technologię, której będziesz używać do identyfikowania, śledzenia, rejestrowania, kategoryzowania i klasyfikowania incydentów. Można użyć rozwiązań UEBA do wykrywania incydentów, UAM do śledzenia i rejestrowania incydentów oraz platform analizy zagrożeń do klasyfikowania incydentów.

Role i obowiązki w różnych scenariuszach incydentów

Zidentyfikuj scenariusze incydentów, które najprawdopodobniej wystąpią w Twojej organizacji i opracuj instrukcje krok po kroku dotyczące obsługi każdego incydentu. Następnie utwórz zespół reagowania na incydenty cyberbezpieczeństwa (CIRT) i przypisz obowiązki jego członkom, aby byli zawsze gotowi do radzenia sobie z incydentami.

Plany dotyczące informowania o incydencie

Twoja organizacja powinna mieć osobę odpowiedzialną za komunikację kryzysową, która zarządza sposobem, w jaki organizacja informuje o incydencie wewnętrznie, a także publicznie i w mediach.

Specjalista ds. komunikacji kryzysowej tworzy również strategię komunikacji, która określa osoby, które muszą zostać poinformowane o incydencie oraz osoby bezpośrednio zaangażowane w proces reagowania na incydent i usuwania jego skutków. Plan musi wyjaśniać, do kogo należy zadzwonić w pierwszej kolejności w przypadku incydentu, kiedy do nich zadzwonić i z kim się skontaktować, jeśli są niedostępni.

Procedury zgłaszania incydentów

Przede wszystkim należy dowiedzieć się, do którego właściwego organu należy się zgłosić. Zapoznaj się z art. 46 DORA, aby dowiedzieć się, do jakiego organu należy się odnieść w zależności od rodzaju organizacji finansowej i uwzględnij go w swoim IRP.

Twoja organizacja musi zgłaszać poważne incydenty odpowiedniemu właściwemu organowi. Zgodnie z wymogami DORA należy przedłożyć:

- Wstępne powiadomienie o incydencie
- Raport cząstkowy
- Istotny raport z aktualizacji statusu (jeśli dotyczy)
- Raport końcowy

Ramy czasowe dla każdego raportu zostaną wkrótce określone w DORA. Różne Europejskie Urzędy Nadzoru są obecnie w trakcie opracowywania standardowych formularzy, szablonów i procedur do wykorzystania przy zgłaszaniu incydentów właściwym organom i oczekuje się, że przedstawią je Komisji Europejskiej do 17 lipca 2024 roku. Bądź na bieżąco.

Działania naprawcze mające na celu złagodzenie skutków incydentu

Opracowanie i udokumentowanie działań wymaganych do opanowania każdego głównego typu incydentu związanego z ICT. Każda strategia powinna obejmować środki ograniczania szkód spowodowanych incydentem, np. zamknięcie systemu lub wyłączenie niektórych funkcji.

Pamiętaj, aby uwzględnić działania, które należy wykonać po opanowaniu incydentu. Na przykład należy określić przepływ pracy i narzędzia do gromadzenia i analizowania informacji podczas identyfikowania pierwotnej przyczyny incydentu, a także przepływ pracy i narzędzia do jej wyeliminowania.

Krok 9. Przeprowadzaj testy cyfrowej odporności operacyjnej

Testowanie odporności jest kluczowym elementem poprawy cyfrowej odporności operacyjnej organizacji i zgodności z DORA. Przeprowadzenie testów cyfrowej odporności operacyjnej pomoże ocenić gotowość do obsługi incydentów związanych z ICT, zidentyfikować luki w odporności operacyjnej i je wyeliminować.

Do czasu przeprowadzenia testów odpornościowych powinieneś mieć mapę wszystkich swoich zasobów informacyjnych i teleinformatycznych. Pomaga to uzyskać pełny obraz zasobów organizacji, połączeń i zależności między nimi oraz krytyczności każdego zasobu.

> Podmioty finansowe, inne niż mikroprzedsiębiorstwa, muszą zapewnić, co najmniej raz w roku, że odpowiednie testy są przeprowadzane na wszystkich systemach ICT i aplikacjach wspierających krytyczne lub ważne funkcje.
>
> **Ustawa o cyfrowej odporności operacyjnej, Artykuł 24 (6)**

Zgodnie z art. 25 (1) podczas przeprowadzania testów odporności organizacje finansowe muszą wdrożyć następujące środki wewnętrznie lub za pośrednictwem zewnętrznych dostawców:

Oceny podatności i skanowanie	Analizy open source	Analizy luk i podatności	Oceny bezpieczeństwa sieci
Kwestionariusze i rozwiązania do skanowania oprogramowania	Przeglądy kodu źródłowego, tam gdzie to możliwe	Testy oparte na scenariuszach	Testowanie kompatybilności
Przeglądy bezpieczeństwa fizycznego	Testowanie wydajności	Testowanie end-to-end	Testy penetracyjne

Wymogi dotyczące przeprowadzania testów cyfrowej odporności operacyjnej zazwyczaj nie mają wpływu na mikroprzedsiębiorstwa. Aby dowiedzieć się, czy mają one zastosowanie do Twojej organizacji, zapoznaj się z rozdziałem IV, w szczególności z art. 25 ust. 3. Jednocześnie niektóre organizacje mogą podlegać obowiązkowi przeprowadzania zaawansowanych testów bezpieczeństwa. Więcej informacji na ten temat znajduje się w art. 26.

Krok 10. Zarządzaj ryzykiem stron trzecich

Aby zachować zgodność z DORA, organizacja finansowa musi poradzić sobie z ryzykiem teleinformatycznym związanym z korzystaniem z usług technologicznych stron trzecich. Zarządzając ryzykiem związanym z korzystaniem z usług podmiotów zewnętrznych, należy pamiętać, że:

- Twoja organizacja finansowa pozostaje w pełni odpowiedzialna za zgodność z DORA, nawet jeśli masz ustalenia umowne dotyczące korzystania z usług ICT stron trzecich
- Należy zarządzać ryzykiem stron trzecich zgodnie z zasadą proporcjonalności, biorąc pod uwagę:
  - Charakter, skala, złożoność i znaczenie zależności technologicznych
  - Wszelkie potencjalne ryzyka wynikające z umów z osobami trzecimi

Zbudowanie skutecznego procesu zarządzania ryzykiem stron trzecich wymaga:

1. Przyjęcia i regularnej weryfikacji strategii dotyczącej ryzyka stron trzecich

Opracowanie i udokumentowanie przemyślanego podejścia do zarządzania ryzykiem związanym z technologiami informacyjno-komunikacyjnymi stron trzecich. Określenie kluczowych działań wymaganych do identyfikacji, oceny i ograniczenia ryzyka związanego z ICT stron trzecich, przydzielenie zasobów do wykonania tych działań i przypisanie obowiązków.

2. Ustanowienia polityki dotyczącej korzystania z krytycznych i ważnych technologii informacyjno-komunikacyjnych stron trzecich

Zapewnienie wytycznych dotyczących korzystania z technologii informacyjno-komunikacyjnych innych firm, które wspierają krytyczne i ważne procesy biznesowe organizacji. Wytyczne te powinny mieć zastosowanie do konkretnych osób (w stosownych przypadkach), określonych grup lub całej organizacji.

3. Prowadzenia rejestru wszystkich ustaleń umownych

Należy prowadzić kompleksowy rejestr całej sieci dostawców usług teleinformatycznych i regularnie go aktualizować. Należy wyraźnie rozróżnić dostawców ICT, którzy wspierają krytyczne funkcje Twojej organizacji, od tych, którzy tego nie robią.

4. Postępowania zgodnie z wytycznymi przed zawarciem umowy

Przed rozpoczęciem korzystania z zewnętrznych usług ICT i podpisaniem umowy należy:

- Określić, czy ta konkretna umowa będzie obejmować technologie informacyjno-komunikacyjne, które wspierają krytyczne lub ważne funkcje organizacji.
- Sprawdzić, czy spełnione są warunki nadzoru nad zawieraniem umów
- Zidentyfikować i ocenić wszystkie ryzyka związane z umową, biorąc pod uwagę możliwość, że umowa ta zwiększy ryzyko zbytniego polegania organizacji na technologii
- Upewnić się, że przeprowadzone zostały wszystkie niezbędne kontrole i oceny, oraz że wybrany dostawca jest odpowiedni
- Przewidywać i oceniać wszelkie konflikty interesów, które może spowodować umowa

Więcej informacji na temat kluczowych postanowień umownych znajduje się w art. 30.

5. Planowanie strategii wyjścia dla kluczowych dostawców technologii

Należy przygotować strategie wyjścia dla dostawców wspierających krytyczne i ważne funkcje organizacji. Mowa tu o znalezieniu alternatywnych rozwiązań i przygotowaniu planów przejścia, które umożliwią Twojej organizacji płynne przeniesienie usług i danych od jednego dostawcy do drugiego.

Musisz zapewnić, że nie wystąpi:

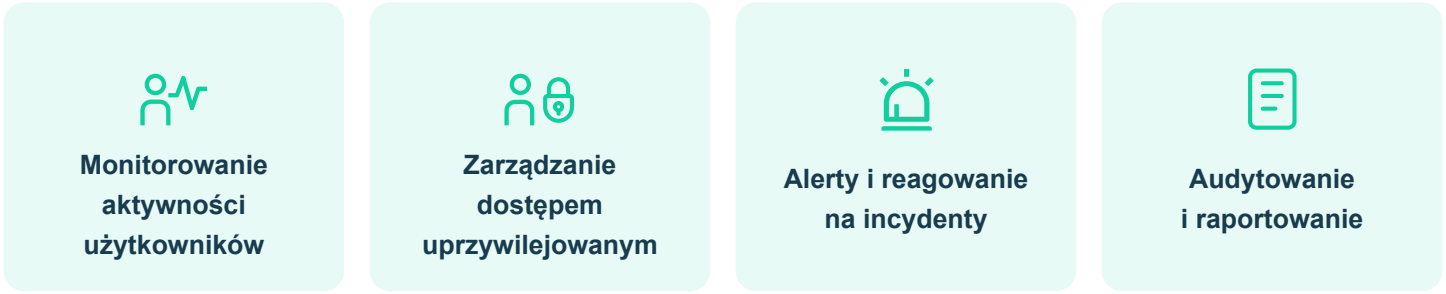
- Zakłócenie działalności biznesowej
- Utrudnianie zgodności z wymogami regulacyjnymi
- Negatywny wpływ na ciągłość i jakość usług świadczonych klientom

Szczegółowe informacje na temat okoliczności, w których umowy muszą zostać rozwiązane, znajdują się w art. 28 (7).

Europejskie Urzędy Nadzoru posiadają uprawnienia do wyznaczania określonych dostawców usług jako krytycznych zewnętrznych dostawców usług ICT dla podmiotów finansowych. Aby dowiedzieć się więcej na temat procesu wyznaczania zewnętrznych dostawców krytycznych usług teleinformatycznych i ram nadzoru nad nimi, zapoznaj się z rozdziałem V, sekcja II.

Uzyskanie zgodności z DORA dzięki Syteca by Ekran System

Syteca by Ekran System to kompleksowe rozwiązanie do zarządzania ryzykiem wewnętrznym, które oferuje kompletny zestaw narzędzi do powstrzymywania ryzyka wewnętrznego, wykrywania zagrożeń i zakłócania incydentów bezpieczeństwa. Wdrażając technologie zarządzania ryzykiem wewnętrznym Syteca, można wykorzystać wiele funkcji:



- **Monitorowanie aktywności użytkowników** umożliwia wgląd i rejestrowanie aktywności użytkowników - pracowników i osób trzecich - w całej infrastrukturze w formacie wideo. Pozwala na przeglądanie na żywo lub nagranych sesji użytkownika z bogatymi metadanymi zapewniającymi kontekst: otwarte aplikacje, odwiedzone strony internetowe, wykonane polecenia, naciśnięcia klawiszy i podłączone urządzenia USB.
- **Zarządzanie dostępem uprzywilejowanym** umożliwia szczegółowe zarządzanie uprawnieniami dostępu wewnętrznego przy jednoczesnym zabezpieczeniu krytycznych punktów końcowych w sieci. Oferuje szeroki zakres funkcji umożliwiających przejęcie kontroli nad dostępem uprzywilejowanym, od zarządzania tożsamością i 2FA do bezpiecznego uwierzytelniania użytkowników po zarządzanie sekretami i sprawdzanie haseł w celu ochrony danych logowania. Przepływ pracy żądania dostępu i zatwierdzania może pomóc w dalszym zwiększeniu ochrony krytycznych systemów.
- **Alerty i reagowanie na incydenty** umożliwiają automatyczne śledzenie i wykrywanie podejrzanych działań w sieci oraz szybkie reagowanie na nie. Konfigurowalne alerty i moduł UEBA oparty na sztucznej inteligencji mogą powiadamiać o podejrzanych zachowaniach użytkowników, podczas gdy funkcja reagowania na incydenty może blokować procesy lub użytkowników po uruchomieniu reguły.
- **Narzędzia do audytu i raportowania** dostarczają wszystkich niezbędnych danych do kompleksowej analizy obecnego środowiska cyberbezpieczeństwa. Syteca by Ekran System oferuje szeroką gamę raportów spełniających określone wymagania. Ponadto płynnie integruje się z Microsoft Power BI, umożliwiając przejrzystą i łatwą prezentację złożonych danych.

Poniżej znajduje się kompleksowy przewodnik szczegółowo opisujący, w jaki sposób Syteca by Ekran System może pomóc Twojej organizacji finansowej w spełnieniu wymagań DORA.

Wspieranie pięciu filarów DORA za pomocą Syteca

Wymóg DORA	Funkcjonalność Syteca
Zarządzanie ryzykiem ICT	• Zwiększ widoczność w swojej sieci dzięki ciągłemu monitorowaniu aktywności • Analizuj wzorce zachowań i oceniaj ryzyko przy użyciu szczegółowych dzienników audytów i raportów • Wykrywaj anomalie w zachowaniu i zauważaj potencjalne zagrożenia dzięki modułowi UEBA od Syteca by Ekran System • Ustaw niestandardowe reguły alertów zgodnie z ustalonymi zasadami bezpieczeństwa i otrzymuj powiadomienia w czasie rzeczywistym
Zarządzanie incydentami związanymi z ICT, ich klasyfikacja i raportowanie	• Wykrywaj szybko incydenty związane z ICT przez otrzymywanie powiadomień o podejrzanych zachowaniach, próbach nieautoryzowanego dostępu i anomaliach systemowych • Przyspiesz proces reakcji na incydenty poprzez automatyzację środków zaradczych, tj. blokady użytkowników czy zabijanie procesu • Ustanów dokładną ścieżkę dowodową w celu zbadania przyczyny, wpływu i zakresu incydentu oraz zapobiegania podobnym przypadkom w przyszłości • Eksportuj zapisy aktywności użytkowników w odpornym na manipulacje formacie pliku, by przesłać dowody dla działań kryminalistycznych • Ujawniaj incydenty związane z bezpieczeństwem i wykazuj zgodność z zasadami bezpieczeństwa odpowiednim organom poprzez bogate w dane i ustrukturyzowane raporty

Wymóg DORA	Funkcjonalność Syteca
Testowanie cyfrowej odporności operacyjnej	• Wzmocnij odporność swojej organizacji przez zarządzanie uprawnieniami dostępu, monitoring aktywności i reagowanie na incydenty • Analizuj wyniki testów odporności, przeglądając raporty informacyjne i dzienniki audytu • Oglądaj sesje użytkowników na żywo podczas testowania odporności, aby analizować wydajność • Wyświetlaj komunikaty ostrzegawcze, aby poinformować użytkowników o niedozwolonych działaniach podczas testów penetracyjnych.
ICT - zarządzanie ryzykiem stron trzecich	• Monitoruj aktywność zewnętrznych dostawców usług na punktach końcowych organizacji, aby zapewnić zgodność z ustalonymi zasadami i standardami bezpieczeństwa • Zdefiniuj szczegółowe uprawnienia dostępu dla dostawców zewnętrznych, zapewniając im dostęp tylko do potrzebnych zasobów i danych • Zwiększ bezpieczeństwo połączeń RDP i szybko wykrywaj nieautoryzowany dostęp do wrażliwych danych oraz wszelkie inne potencjalnie złośliwe działania • Konfiguruj niestandardowe alerty na żywo oraz powiadomienia o podejrzanych zachowaniach i naruszeniach bezpieczeństwa użytkowników zewnętrznych • Nadzoruj aktywność zewnętrznych dostawców w infrastrukturze IT za pomocą szczegółowych dzienników aktywności użytkowników
Wymiana informacji i danych	• Rejestruj szczegółowe zapisy aktywności użytkowników i dokumentuj incydenty bezpieczeństwa, by udostępniać je organom regulacyjnym i innym podmiotom finansowym na potrzeby zgłaszania incydentów i współpracy • Generuj kompleksowe dzienniki i raporty w celu wykazania zgodności z wymogami regulacyjnymi w zakresie cyberbezpieczeństwa • Eksportuj dane w chronionym formacie pliku

Case studies

Zapewnienie zgodności i zarządzanie ryzykiem wewnętrznym za pomocą Syteca by Ekran System

Historia sukcesu klienta

Cecabank zapewnia zgodność z przepisami dzięki Syteca by Ekran System

Wyzwanie

Ze względu na ciągłą pracę z danymi finansowymi swoich klientów, Cecabank musi przestrzegać ścisłych kontroli bezpieczeństwa. Aby zachować zgodność i poprawić cyberbezpieczeństwo, nasz klient musiał zmniejszyć ryzyko naruszenia bezpieczeństwa konta SWIFT i wykryć potencjalne wykorzystanie naruszonych danych uwierzytelniających SWIFT.

Cecabank poszukiwał wiarygodnego partnera, który pomógłby mu spełnić wymogi regulacyjne. Po zbadaniu rynku zdecydowali się na Ekran System.

Rozwiązanie

Oto, jak Cecabank zdołał zwiększyć cyberbezpieczeństwo i spełnić wymogi regulacyjne za pomocą Syteca:

- Ugruntowano widoczność w środowisku SWIFT
- Wdrożono proces wykrywania użycia naruszonych danych uwierzytelniających SWIFT
- Zapewniono łatwą i wydajną analizę danych dzięki przekazywaniu dzienników dostępu SWIFT do systemu SIEM

Rezultat

Cecabank zdołał zwiększyć cyberbezpieczeństwo i spełnić wymogi regulacyjne za pomocą Syteca poprzez:

- ✓ Zrozumienie, kto i co robi w środowisku SWIFT
- ✓ Zapobieganie lub powstrzymywanie ataków w środowisku SWIFT na wczesnych etapach
- ✓ Łatwą analizę dzienników dostępu SWIFT za pośrednictwem SIEM

> Część funkcjonalności Syteca pozwoliła nam zrealizować cele związane z bezpieczeństwem. Teraz monitorowanie i audyt użytkowników uzyskujących dostęp do sieci SWIFT za pośrednictwem naszego środowiska jest znacznie łatwiejsze.
>
> **Architekt Bezpieczeństwa**
> Cecabank

Przejdź tu,
aby przeczytać całą historię klienta

Historia sukcesu klienta

VakifBank zarządza działaniami stron trzecich i administratorów na serwerze terminalowym za pomocą Syteca by Ekran System

Wyzwanie

Zapewnienie bezpieczeństwa danych finansowych wymagało od VakifBank jednoczesnego nadzorowania zarówno administratorów, jak i podwykonawców na serwerach terminali. W tamtym czasie zadanie to stanowiło szczególne wyzwanie dla naszego klienta. Jako międzynarodowa korporacja, VaktifBank potrzebował więc sposobu na zarządzanie nieograniczoną liczbą uprzywilejowanych użytkowników. Ponadto, musieli spełnić tureckie i międzynarodowe wymogi cyberbezpieczeństwa IT w sferze bankowości.

Przed skontaktowaniem się z nami, VakifBank wypróbował inne rozwiązania do monitorowania aktywności użytkowników, ale wciąż przekraczały one budżet. Szukali więc alternatywy i trafili na Syteca by Ekran System jako oprogramowanie o najwyższym stosunku możliwości technicznych do ceny.

Rozwiązanie

Z pomocą Syteca, VakifBank zdołał sprostać wyzwaniom związanym z cyberbezpieczeństwem. Podczas realizacji:

- Ustanowiono zarządzanie użytkownikami uprzywilejowanymi na serwerach terminali
- Wdrożono proces monitorowania aktywności administratorów i zewnętrznych kontrahentów
- Umożliwiono nagrywanie sesji użytkowników i ich długotrwałe przechowywanie
- Usprawniono procesy raportowania zdarzeń bezpieczeństwa i audytu zgodności
- Umożliwiono nadzór nad nieograniczoną liczbą użytkowników, przy jednoczesnym zachowaniu budżetu przeznaczonego na cyberbezpieczeństwo

Rezultat

Korzystając z wielu możliwości Syteca by Ekran System, VakifBank zwiększył swoje cyberbezpieczeństwo na serwerach terminali i otrzymanych danych przez:

- ✓ Scentralizowaną i szybką konfigurację uprawnień dostępu
- ✓ Pełny wgląd w aktywność administratorów i stron trzecich
- ✓ Możliwość nagrywania sesji użytkownika i przechowywania ich przez długi czas
- ✓ Zaawansowany proces audytu bezpieczeństwa i zgodności

Przejdź tu,
aby przeczytać całą historię klienta.

Historia sukcesu klienta

Bank Europejski uzyskuje zgodność z DORA oraz przeciwdziała zagrożeniom wewnętrznym dzięki Syteca by Ekran System

Wyzwanie

Wraz z rozwojem organizacji naszego klienta, monitorowanie infrastruktury i ochrona wrażliwych danych za pomocą istniejącego oprogramowania stawały się coraz większym wyzwaniem. Dlatego zaczęli szukać bardziej skalowalnego i łatwiejszego w użyciu rozwiązania cyberbezpieczeństwa, które pomogłoby im wykonać następujące zadania:

- Zapewnić bezpieczeństwo wrażliwych danych
- Uzyskać zgodność z wymaganiami IT i korporacyjnymi politykami
- Przeprowadzać szybkie audyty
- Wykrywać i powstrzymywać zagrożenia wewnętrzne

Klient ten spędził wcześniej pół roku testując oprogramowanie, aby jak najlepiej spełnić swoje potrzeby. Po dokonaniu oceny kilku rozwiązań monitorujących, wybrał Syteca by Ekran System.

Rozwiązanie

Oto jak wykorzystali funkcjonalności Syteca by Ekran System, aby wyjść naprzeciw swoim potrzebom:

- Zapewniono bezpieczne przetwarzanie danych na serwerach terminali
- Usprawniono proces spełniania wymogów bezpieczeństwa IT
- Zoptymalizowano audyty wewnętrzne
- Wdrożono proces wykrywania i zakłócania złośliwej działalności osób mających dostęp do informacji poufnych

Rezultat

Po wdrożeniu byli w stanie:

- ✓ Uzyskać wgląd w aktywność użytkowników na serwerach terminali
- ✓ Zapewnić szybkie i skuteczne audyty wewnętrzne
- ✓ Utrzymać zgodność z wymogami cyberbezpieczeństwa
- ✓ Wykrywać i zatrzymywać szkodliwe działania w czasie rzeczywistym

Przejdź tu,
aby poznać całą historię klienta.

Podsumowanie

Przed wprowadzeniem DORA przepisy dotyczące zarządzania ryzykiem dla instytucji finansowych w UE miały głównie na celu sprawdzenie, czy organizacje utrzymują wystarczający kapitał, aby złagodzić ryzyko operacyjne. Poprzez DORA, UE próbuje zmienić to podejście i wprowadza uniwersalne ramy zarządzania ryzykiem ICT w sektorze finansowym.

Zgodność z przepisami DORA może stanowić wyzwanie dla Twojej organizacji, ale dzięki odpowiedniemu podejściu i dedykowanym narzędziom będziesz w stanie osiągnąć swój cel. W rezultacie nie tylko spełnisz wymagania DORA, ale także zwiększysz bezpieczeństwo swojej organizacji.

Syteca by Ekran System to kompleksowa platforma do zarządzania ryzykiem wewnętrznym z licznymi funkcjami zwiększającymi cyberbezpieczeństwo organizacji. Wykorzystując bogaty zestaw funkcjonalności Syteca by Ekran System, można:

- **Kontrolować dostęp do zasobów**
- **Weryfikować tożsamość użytkowników**
- **Monitorować aktywność**
- **Wykrywać zdarzenia bezpieczeństwa i reagować na nie**
- **Zgłaszać i badać incydenty**
- **Bezpiecznie współpracować z osobami trzecimi**
- **Ograniczać ryzyko wewnętrzne**

Skontaktuj się z nami, aby dowiedzieć się więcej o Syteca oraz o tym, w jaki sposób rozwiązanie może usprawnić Twoje działania. Zapytaj o dostęp do portalu demonstracyjnego, aby zobaczyć, co Syteca ma do zaoferowania, lub przetestować jej możliwości w ramach bezpłatnego 30-dniowego okresu próbnego.

Zwiększ swoją cyfrową odporność operacyjną dzięki Syteca, która spełnia wymagania DORA

Odwiedź www.syteca.com lub skontaktuj się z nami przez email: biuro@securivy.com

Syteca
formerly Ekran System