SECUREVISIO

Szpital zgodny z KSC, RODO oraz KRI

Jak z wykorzystaniem SecureVisio podnieść poziom cyberbezpieczeństwa

Szpitale stoją przed szansą, ale i wyzwaniem podniesienia poziomu cyberbezpieczeństwa dla swoich kluczowych procesów i usług. Ustawa o Krajowym Systemie Cyberbezpieczeństwa *(UoKSC)*, Rozporządzenie o Ochronie Danych Osobowych *(RODO)* i Rozporządzenie ws. Krajowych Ram Interoperacyjności *(KRI)* wskazują wiele obszarów, które muszą zostać zaadresowane przez dostawcę usług kluczowych w celu spełnienia wymogów ustawowych. System SecureVisio, jako zintegrowana platforma do kompleksowego i efektywnego zarządzania bezpieczeństwem, umożliwia spełnienie tych wymogów.

Obowiązki Operatora Usługi Kluczowej adresowane za pomocą systemu SecureVisio (oznaczone w tabeli kolorem szarym)

W terminie 3 miesięcy	W terminie 6 miesięcy	W terminie 12 miesięcy
Dokonuje szacowania ryzyka dla swoich usług kluczowych	Wdraża odpowiednie i adekwatne do oszacowanego ryzyka środki techniczne i organizacyjne	Przygotowuje pierwszy audyt w rozumieniu ustawy
Zarządza incydentami	Zbiera informacje o zagrożeniach i podatnościach	
Wyznacza osobę kontaktową z właściwym CSIRT i organem właściwym do spraw cyberbezpieczeństwa	Stosuje środki zapobiegające i ograniczające wpływ incydentów na bezpieczeństwo systemu informacyjnego	
Prowadzi działania edukacyjne wobec użytkowników	Stosuje wymaganą dokumentację	Przekazuje sprawozdanie z audytu wskazanym w ustawie podmiotom
Obsługuje incydenty we własnych systemach		
Zgłasza incydenty poważne		
Usuwa wskazane podatności		

Kompleksowe zarządzanie cyberbezpieczeństwem w SecureVisio odbywa się na trzech płaszczyznach:
PREWENCJI, DETEKCJI oraz REAKCJI *(PDR)*.

- W ramach **PREWENCJI** SecureVisio pozwala automatycznie stworzyć i utrzymać centralną e-dokumentację zasobów IT *(funkcjonalność CMDB – Configuration Management Database)*, prowadzić analizę ryzyka cyberzagrożeń *(narzędzia klasy IRM – Integrated Risk Management)* oraz zarządzać podatnościami z uwzględnieniem kluczowych procesów i zasobów organizacji *(mechanizm TVM – Threat and Vulnerability Management).*
- Z perspektywy **DETEKCJI**, SecureVisio wspomaga użytkowników w wykrywaniu zaawansowanych zagrożeń poprzez działanie kontekstowych reguł korelacyjnych *(funkcjonalność SIEM – Security Information and Event Management)* oraz wykrywania anomalii w zachowaniu użytkowników oraz systemów *(narzędzie klasy UEBA – User and Entity Behavior Analysis).*
- W obszarze **REAKCJI** platforma SecureVisio dostarcza gotowe, automatyczne scenariusze reakcji, które pozwalają szybko obsłużyć wykryte zagrożenia *(funkcjonalność typu SOAR – Security Automation and Response).*

SECUREVISIO

Wymogi regulacji UoKSC, RODO oraz KRI

Główne wymagania	UoKSC	SECUREVISIO	RODO	SECUREVISIO	KRI	SECUREVISIO
szacowania ryzyka dla usług krytycznych	Art. 17 pkt 2	✓				
szacowania ryzyka dla osoby fizycznej			Art. 32 pkt 1	✓		
szacowania ryzyka dla rejestrów publicznych, systemów informatycznych oraz wymiany informacji w postaci cyfrowej					§ 4 pkt 2	✓
wdrożenia adekwatnych do wyników szacowania ryzyka środków technicznych	Art. 17 pkt 2 i 3	✓	Art. 32 pkt 2	✓		
identyfikowania i usuwania podatności	Art. 18 pkt 1 ppkt 6	✓			§ 20 pkt 12 lit. f i g	✓
wykrywania incydentów, klasyfikowania ich oraz obsługi	Art. 18 pkt 1 ppkt 1-5	✓				
zgłaszanie naruszeń bezpieczeństwa	Art. 18 pkt 2	✓	Art. 33	✓	§ 20 pkt 13	✓
prowadzenia dokumentacji zgodnej ze zdefiniowanymi wymaganiami	Art. 10 pkt 1-3	✓	Art. 30	✓	§ 15 pkt 2	✓

SecureVisio integruje wszystkie wymienione funkcjonalności, pozwalając użytkownikowi z perspektywy jednej konsoli na szacowanie ryzyka wystąpienia incydentu, zarządzanie tym ryzykiem, zarządzanie samymi incydentami i podatnościami, obsługę incydentu i podatności oraz przekazanie dostępu do informacji o rejestrowanych incydentach właściwym zespołom reagowania na incydenty (CSIRT MON, CSIRT NASK, CSIRT GOV).

Wdrożenie systemu SecureVisio zapewni spełnienie wymagań zdefiniowanych w UoKSC, RODO oraz KRI poprzez:

- Zapewnienie wymaganej dokumentacji, pozwalającej m.in. na:
  - Opis zastosowanych środków technicznych i organizacyjnych;
  - Procedury, instrukcje, inwentaryzację systemów i usług krytycznych;
  - Rejestry, w tym także rejestr czynności przetwarzania;
  - Plany ciągłości działania;
- Automatyczne zarządzanie ryzykiem przetwarzania danych i usług kluczowych;
- Automatyczną ocenę skutków przetwarzania w systemach informatycznych;
  - Względem poufności, integralności i dostępności danych oraz świadczonych usług;
  - Względem osoby fizycznej (DPIA);
- Automatyczną prewencję, detekcję i reakcję;
  - Zarządzanie podatnościami;
  - Zarządzanie incydentami;
- Zapewnienie wiedzy oraz narzędzi dla wyznaczonej osoby kontaktowej.

SECUREVISIO

Dodatkowe możliwości jakie oferuje SecureVisio w zakresie cyberbezpieczeństwa dla szpitali:

- **Analiza ryzyka cyberzagrożeń** – SecureVisio buduje w organizacji świadomość ryzyka związanego z cyberzagrożeniami, co pozwala na efektywne wykorzystanie zabezpieczeń. Platforma obejmuje mechanizmy automatycznej i dynamicznej analizy ryzyka cyberzagrożeń dla procesów i zasobów, z wykorzystaniem danych zgromadzonych na etapie inwentaryzacji, tj. tworzenia automatycznej e-dokumentacji w postaci mapy logicznej infrastruktury IT. Mapa ta jest na bieżąco i automatycznie aktualizowana przez SecureVisio i rozwija się razem z organizacją.
- **Gromadzenie i przechowywanie informacji o zdarzeniach z całej infrastruktury IT** – SecureVisio przechowuje logi, koreluje zdarzenia z różnych urządzeń i wykrywa potencjalne nieprawidłowości, dzięki wbudowanym regułom korelacyjnym oraz algorytmom uczenia maszynowego. Wbudowane, automatyczne mechanizmy archiwizacji umożliwiają długotrwałe, centralne lub rozproszone, przechowywanie danych na wskazanej przestrzeni dyskowej.
- **Implementacja procesu obsługi incydentów** - pozwalająca na ocenę czy zdarzenie, którym się zajmujemy stanowi realne zagrożenie lub czy jest to wyłącznie fałszywy alarm. Każdy potencjalny incydent lub podatność staje się elementem procesu, w ramach którego, SecureVisio automatycznie wzbogaca dane, śledzi status, czas reakcji i obsługi, eskaluje, bada potencjalne konsekwencje oraz dostarcza scenariusze postępowania na każdym etapie analizy i reakcji.
- **Kompleksowe oraz kontekstowe podejście do obsługi podatności** - m.in. poprzez automatyczne ustalanie ich priorytetu, przydzielanie scenariuszy obsługi, przypisanie zadań członkom zespołu odpowiedzialnego za zarządzanie podatnościami, śledzenie czasów reakcji i obsługi oraz eskalację.
- **Automatyzacja i orkiestracja** – system automatyzuje czynności związane z obsługą zdarzeń, incydentów oraz podatności, w związku z czym umożliwia realne i natychmiastowe podniesienie poziomu bezpieczeństwa w organizacji, bez zwiększenia nakładów pracy i konieczności angażowania ekspertów. Moduł obsługi incydentów zawiera gotowe scenariusze i setki akcji, które pozwalają na automatyczne lub zautomatyzowane interakcje z zewnętrznymi systemami w ramach prac związanych z uzupełnianiem informacji, pivotingiem oraz reakcją na incydenty oraz podatności.
- **Ochrona danych osobowych** - pozwalająca na spełnienie wymogów RODO poprzez dostarczenie:
  - pełnej analizy ryzyka utraty poufności, dostępności oraz integralności danych wraz z możliwością raportowania i oceny skutków dla ochrony danych osobowych (Art. 35) oraz raportowania naruszeń dla organu nadzorczego (Art. 33 ust. 3);
  - automatycznej analizy ryzyka cyberzagrożeń dla zasobów przetwarzających dane osobowe;
  - możliwości tworzenia i prowadzenia Rejestrów Czynności Przetwarzania (RCP) i Rejestrów Kategorii Czynności Przetwarzania (RKCP) zgodnie z Art. 30, Rejestru Upoważnień (Art. 32 ust. 4), Rejestru Umów Powierzeń (Art. 28), Rejestru Udostępnień (Art. 5), Rejestru Naruszeń (Art. 33 ust. 5), Rejestru Wniosków i Rozszczeń (Art. 15 i 16), Rejestru Szkoleń.

SECUREVISIO

SECUREVISIO

Podsumowanie korzyści dla szpitali:

- Zintegrowna platforma do zarządzania bezpieczeństwem z wbudowanymi i gotowymi do użycia narzędziami do PREWENCJI, DETEKCJI I REAKCJI (PDR) względem kluczowych zagrożeń;
- Szerokie pokrycie wymagań prawnych: UoKSC, RODO, KRI – pełna zgodność z kluczowymi wytycznymi dla jednostek publicznych w zakresie cyberbezpieczeństwa;
- Zgodność systemu z metodykami: ISO27001, ISO27005, ISO27035;
- SecureVisio jako optymalna inwestycja w bezpieczeństwo IT – wbudowane w system narzędzia klasy: CMDB, IRM, SIEM, UEBA, SOAR, TVM elmininują konieczność indywidualnych zakupów i wdrożeń wspomnianych systemów oraz utrzymania ich wzajemnej, kosztownej i długotrwałej integracji;
- Lokalne wsparcie posprzedażowe w zakresie utrzymania systemu – dedykowany konsultant producenta do dyspozycji klientów przez cały okres wsparcia;
- Interfejs systemu w języku polskim i angielskim – czytelny i przejrzysty sposób prezentacji danych;
- Wdrożenia w organizacjach służby zdrowia – system sprawdzony w realiach pracy szpitali;
- Szybkie i nieangażujące użytkowników wdrożenie – już w pierwszym miesiącu instalacji system skutecznie podnosi poziom bezpieczeństwa organizacji;
- Elastyczne i korzystne licencjonowanie oparte o model licencji wieczystej;
- Optymalizacja wydatków na bezpieczeństwo – wdrożenie matrycy analizy ryzyka pozwala obiektywnie i racjonalnie spojrzeć na konieczność zakupu nowych techonologii bezpieczeństwa (zobrazowanie ryzyk dla kluczowych procesów);
- Priorytetyzacja z wykorzystaniem kontekstu – wbudowane narzędzia inwentaryzacji zasobów i procesów IT w połączeniu z silnikiem analizy ryzyka, pozwalają operatorom skoncentrować się na kluczowych zagrożeniach i wykorzystać dostępny czas na obsługę najważniejszych alarmów;
- SecureVisio jako „Centrum Bezpieczeństwa" – system stanowi repozytorium wiedzy organizacji – zarówno pod kątem infrastrukturalnym, procesowym jak i operacyjnym. Użytkownicy z poziomu jednego narzędzia mają dostęp do elektronicznej dokumentacji, analizy ryzyka cyberzagrożeń, przeglądarki logów bezpieczeństwa, widoku obsługi incydentów, podatności oraz obszaru zarządzania danymi osobowymi;
- Automatyzacja zarządzania incydentami i podatnościami – SecureVisio jako „wirtualny asystent bezpieczeństwa". System automatyczne weryfikuje zdarzenia, przeprowadzając pierwszą weryfikację, a następnie w przypadku wykrycia poważnego zagrożenia informuje użytkowników, wysyłając odpowiednie powiadomienia. Wykorzystanie gotowych scenariuszy obsługi incydentów i podatności oraz wbudowanej w system wiedzy sprawia, że SecureVisio jest skutecznym i nieocenionym wsparciem eksperckim dla operatorów.

W opinii Naszego Klienta

„SecureVisio stanowi trzon naszego SOC. Od dwóch lat intensywnie korzystamy z tego produktu i nie wyobrażamy sobie teraz pracy w obszarze operacyjnym, a także w wykrywaniu incydentów i zdarzeń bez SecureVisio. To jest narzędzie, które w sposób optymalny pozwala na podniesienie poziomu bezpieczeństwa w każdej organizacji, w tym u operatorów usług kluczowych. Daje szpitalom szansę na efektywne i pełne uzupełnienie braków w cyberbezpieczeństwie."

Michał Hordejuk
Konsultant ds. Cyberbezpieczeństwa
Nowy Szpital Wojewódzki Sp. z o.o. we Wrocławiu