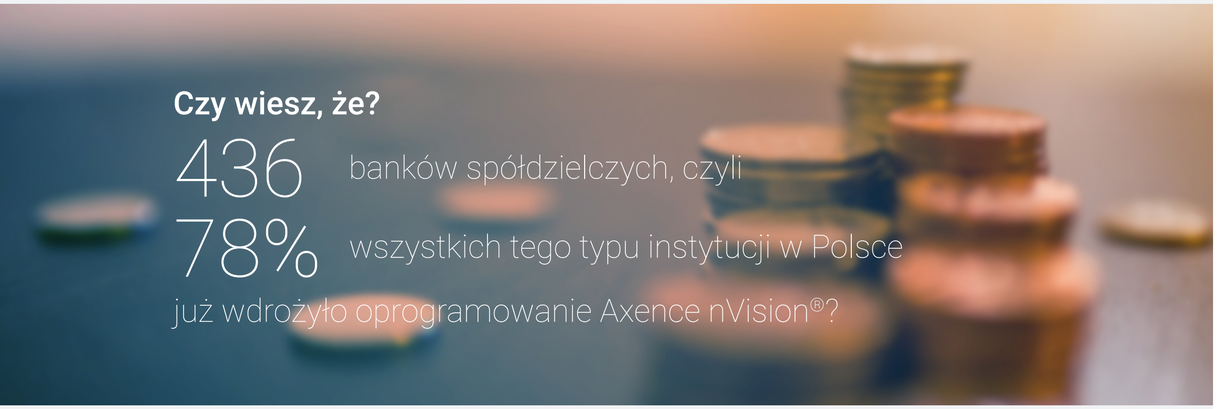
Bezpiecznie jak w banku z Axence nVision®

Oprogramowanie Axence nVision® pomaga spełnić wytyczne Komisji Nadzoru Finansowego z zakresu zarządzania i bezpieczeństwa IT w bankach (tzw. Rekomendacja D).



Czy wiesz, że?

436 banków spółdzielczych, czyli

78% wszystkich tego typu instytucji w Polsce

już wdrożyło oprogramowanie Axence nVision®?

Platforma Axence nVision® odpowiada na szereg potrzeb związanych z zarządzaniem technologią informacyjną i bezpieczeństwem środowiska teleinformatycznego w instytucjach finansowych:

- pomaga w stworzeniu i realizacji polityki bezpieczeństwa,
- monitoruje sieć pod kątem potencjalnych awarii,
- umożliwia kontrolę legalności oprogramowania,
- realizuje audyt i rozlicza wykorzystanie licencji,
- chroni przed nieautoryzowanym działaniem pracowników,
- usprawnia działanie pomocy technicznej,
- zabezpiecza dane przed wyciekiem.

Czytaj Case Study

Dowiedz się więcej:

Napisz na sprzedaz@axence.net, zadzwoń +48 12 426 40 35

lub skontaktuj się z jednym z Autoryzowanych Partnerów Axence.

Rekomendacje KNF, które pomaga spełnić Axence nVision®

Nr	Bank powinien:	nVision axence®
1	nadzorować funkcjonowanie obszarów technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego	monitoruje infrastrukturę sieciową i pozwala podnieść poziom bezpieczeństwa IT
2	posiadać sformalizowany system informacji zarządczej (...) zapewniający każdemu z odbiorców informacji właściwy poziom wiedzy o tych obszarach	pozwala generować szczegółowe dane o stanie infrastruktury sieciowej oraz aktywności użytkowników końcowych
7	rozwijać systemy IT w sposób zapewniający wsparcie jego działalności oraz uwzględniający wymogi bezpieczeństwa środowiska teleinformatycznego	pozwala zdiagnozować potrzebę zakupu nowego sprzętu lub oprogramowania, oraz identyfikuje „wąskie gardła" w sieci
8	posiadać sformalizowane zasady zarządzania danymi wykorzystywanymi w ramach prowadzonej działalności, obejmujące w szczególności zarządzanie architekturą oraz jakością danych (...)	realizuje funkcje zarządzania jakością danych m.in. przez blokowanie odczytu/zapisu plików o określonych rozszerzeniach np. .avi, .mp3 itd., a także przez blokowanie uruchamiania określonych aplikacji przez użytkowników końcowych
9	posiadać sformalizowane zasady dotyczące zarządzania infrastrukturą teleinformatyczną, w tym jej architekturą, poszczególnymi komponentami, wydajnością i pojemnością oraz dokumentacją (...)	umożliwia automatyczne wykrywanie sieci, monitorowanie urządzeń (w tym bankomatów), inwentaryzację sprzętową i programową, a także kontrolę dostępu do nośników danych
11	posiadać mechanizmy techniczne zapewniające właściwy poziom kontroli dostępu logicznego do danych i informacji (...)	pozwala stworzyć politykę dostępu do danych umieszczonych na zewnętrznych nośnikach
12	zapewnić odpowiednią ochronę środowiska teleinformatycznego przed szkodliwym oprogramowaniem	posiada szereg funkcji uzupełniających łańcuch bezpieczeństwa firmy, takich jak np. monitorowanie i alarmowanie o podejrzanych wpisach w harmonogramie zadań Windows
13	zapewniać wewnętrznym użytkownikom systemów informatycznych wsparcie w zakresie rozwiązywania problemów związanych z ich eksploatacją, w tym wynikających z wystąpienia awarii iinnych niestandardowych zdarzeń zakłócających ich użytkowanie	oferuje nowoczesny, funkcjonalny helpdesk dostępny z poziomu przeglądarki internetowej
17	posiadać sformalizowane zasady zarządzania tzw. oprogramowaniem użytkownika końcowego, skutecznie ograniczające ryzyko związane z eksploatacją tego oprogramowania	przez moduł inwentaryzacji sprawuje kontrolę nad legalnością oprogramowania zainstalowanego na komputerach użytkowników końcowych. Dodatkowo monitoruje jakie aplikacje są wykorzystywane najczęściej
18	prowadzić (...) działania związane z identyfikacją, szacowaniem, kontrolą, przeciwdziałaniem, monitorowaniem i raportowaniem ryzyka (...)	zapewnia stały monitoring sieci i użytkowników wraz z systemem alarmów i akcji korekcyjnych
21	zapewnić zgodność funkcjonowania obszarów technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego z wymaganiami prawnymi, regulacjami wewnętrznymi i zewnętrznymi, zawartymi umowami i przyjętymi w banku standardami	przez monitorowanie aktywności użytkowników skutecznie egzekwuje przestrzeganie zasad polityki bezpieczeństwa i wewnętrznych procedur. Możliwe jest blokowanie dostępu do potencjalnie niebezpiecznych treści oraz kontrola legalności oprogramowania