

CyberCheck

BEZPIECZNA INFRASTRUKTURA BANKU SPÓŁDZIELCZEGO

W odpowiedzi na rosnące ryzyko cyberzagrożeń w sektorze finansowym, zespół ekspertów Verdit przygotował pakiet kluczowych rozwiązań bezpieczeństwa dla Banków Spółdzielczych. Dzięki nim skutecznie zabezpieczysz swój Bank przed najpopularniejszymi formami zagrożeń cyfrowych, m.in.: malware, ataki wykorzystujące podatności, phishing, ransomware czy spoofing.

Rozwiązania bezpieczeństwa Verdit pozwalają także na spełnienie wymagań regulatora w zakresie np. Rozporządzenia w sprawie operacyjnej odporności cyfrowej (DORA), Rekomendacji D lub Wytycznych EBA wymaganych przez KNF.

4

KROKI DO ZABEZPIECZENIA BANKU

KROK
01

AUDYT

Na początku nasi eksperci przyjrzą się dokładnie wszystkim kluczowym elementom infrastruktury Twojego Banku i zidentyfikują potencjalne zagrożenia. To niczym wizyta lekarska, na której zbieramy wszystkie niezbędne informacje i przeprowadzamy szczegółowe badania.

KROK
02

RAPORT BEZPIECZEŃSTWA

Opracowujemy kompleksowy dokument opisujący wszystkie zagrożenia i nieprawidłowości. Rekomendujemy też działania naprawcze. Ten raport pomoże Ci także w wywiązaniu się z zaleceń rekomendacji KNF. Jest to kompleksowy i indywidualny plan profilaktyki cyberzagrożeń Twojego Banku.

KROK
03

WYBÓR ROZWIĄZAŃ

Wiesz już, co może stanowić potencjalne zagrożenie. Teraz czas na wybór konkretnych usług. Choć ostateczna decyzja należy do Ciebie, to nasi eksperci są cały czas do Twojej dyspozycji i chętnie odpowiedzą na wszelkie pytania.

KROK
04

WDROŻENIE

Przechodzimy do działania! Wspólnie wdrażamy wybrane usługi, realizując dopasowaną strategię bezpieczeństwa Twojego Banku.

Verdit

Zaufany partner Banków Spółdzielczych

Jesteśmy architektem i integratorem rozwiązań informatycznych dla sektora finansowego, głównie Banków Spółdzielczych. Od blisko 15 lat świadczymy kompleksowe rozwiązania IT oraz przybliżamy świat nowych technologii. Zaufało nam już ponad 350 Klientów.



www.verdit.pl



WYBIERZ ROZWIĄZANIA DLA TWOJEGO BANKU



BADANIE PODATNOŚCI SYSTEMÓW INFORMATYCZNYCH

Kompleksowe rozwiązanie w zakresie identyfikacji i klasyfikacji podatności występujących w systemach informatycznych. Po wykonaniu usługi przekazujemy precyzyjny raport techniczny zawierający informacje o zbadanych urządzeniach, wykrytych podatnościach oraz poziomie ich krytyczności, a także sugerowane działania naprawcze.



SEJF HASEŁ

Oprogramowanie centralizujące zarządzanie hasłami i danymi dostępowymi do różnych systemów i portali. W sposób bezpieczny i zorganizowany automatyzuje pracę oraz minimalizuje ryzyko nieupoważnionego dostępu. Program obsługuje różne typy danych jak: loginy, hasła, klucze API, czy MS Authenticator.



OCHRONA INFRASTRUKTURY WEWNĘTRZNEJ

System chroniący wewnętrzną sieć bankową przed połączeniem nieautoryzowanych urządzeń, zgodnie z protokołem 802.1x. Zachowując ten standard tylko zweryfikowani użytkownicy oraz sprzęty mogą otrzymać dostęp do infrastruktury sieciowej.



MONITORING INFRASTRUKTURY BANKU SPÓŁDZIELCZEGO

Służy do zbierania, analizowania i wizualizacji danych. Pozwoli wykryć wszelkie odchylenia od normy w infrastrukturze IT, gwarantując wczesne wykrycie, diagnozę i rozwiązanie występujących problemów.



BEZPIECZEŃSTWO STACJI ROBOCZYCH

Zapewnia zgodność z regulacjami i wewnętrznymi przepisami Banku, dając kontrolę nad punktami końcowymi w sieci. Umożliwia bezpieczną, zdalną łączność z infrastrukturą Banku (VPN), realizowaną z poziomu łatwej w obsłudze aplikacji klienta.



MONITOROWANIE SESJI ZDALNYCH

Pozwala na ścisłą kontrolę działań użytkowników, także tych o podwyższonych uprawnieniach oraz dostawców usług, zarówno w kontekście bezpieczeństwa, jak i zgodności z regulacjami.



USŁUGA DORADZTWA PRAWNEGO

Usługa dostosowania umów do wymogów prawnych wynikających z rozporządzenia DORA. Weryfikacja dokumentacji bankowej wraz z identyfikacją luk prawnych oraz rekomendacją zmian. Dostosowanie umów z dostawcami usług ICT do zapisów DORA.



AUDYT LICENCJI ORAZ UMÓW

Inwentaryzacja licencji Banku w zakresie posiadanego sprzętu i oprogramowania, ze szczególnym uwzględnieniem Platformy Microsoft 365. Może obejmować także audyt zawartych umów w zakresie łącz do internetu, wsparcia na sprzęt oraz licencji na oprogramowanie do zarządzania infrastrukturą.