Polityka dotycząca cyberbezpieczeństwa

Cele i zakres dokumentu

Celem polityki z zakresu cyberbezpieczeństwa jest ochrona danych i infrastruktury IT Grupy Kapitałowej przed cyberzagrożeniami i ich nieuprawnionym wykorzystaniem. Regulacja ta określa wymogi dotyczące cyberbezpieczeństwa i podkreśla rolę wszystkich pracowników w tym zakresie – nie tylko specjalistów, ale wszystkich użytkowników bankowych rozwiązań IT. Polityka podlega dorocznemu przeglądowi i ewentualnej aktualizacji. Towarzyszą jej liczne dokumenty operacyjne.

Jakie zagadnienia związane z ESG opisuje polityka?

Polityka określa środki, jakie Grupa Kapitałowa stosuje, żaby chronić się przed cyberzagrożeniami. Grupa Kapitałowa stale udoskonala rozwiązania w zakresie cyberbezpieczeństwa i stosuje najlepsze z dostępnych rozwiązań technologicznych, dopasowane do poziomu i rodzaju ryzyk występujących w danej sytuacji. Obejmuje to technologie takie jak: szyfrowanie, anonimizacja danych, zapory sieciowe, blokowanie podejrzanych wiadomości, zarządzanie tożsamością cyfrową, uwierzytelnianie wieloczynnikowe i inne. Określone w polityce wymogi w zakresie ochrony infrastruktury IT obejmują m.in.:

- konfigurację bezpieczeństwa systemów i usług IT, a także mechanizmy kontrolne w tym zakresie, oraz zarządzanie instalacjami poprawek,
- ochronę sieci na potrzeby zapobiegania i powstrzymywania ataków cybernetycznych oraz ograniczania ich skutków.

W zakresie bezpieczeństwa informacji polityka określa wytyczne dotyczące przetwarzania, przechowywania i transmisji danych, które mają na celu ich ochronę przed modyfikacją, utratą, ujawnieniem czy niedozwolonym dostępem. Dodatkowe wymogi dotyczą przetwarzania informacji w chmurze. Dla różnych klas danych Grupa Kapitałowa określa minimalny poziom bezpieczeństwa. Ze względu na poziom poufności dane są klasyfikowane m.in. jako publiczne, wrażliwe i ściśle chronione. Przy określaniu poziomu ochrony danych bierze się pod uwagę uwarunkowania biznesowe i regulacyjne, w tym te dotyczące ochrony danych osobowych, tajemnicy bankowej i innych informacji niejawnych. Dla poszczególnych aktywów IT zostały określone uprawnienia dostępu dla wszystkich ról funkcjonalnych. Polityka opisuje zasady okresowego przeglądu dostępów oraz podział odpowiedzialności w zakresie kluczowych kontroli. Dokument opisuje wymagania w zakresie zarządzania tożsamością użytkowników i dostępem do tych danych. Działania te służą zapewnieniu poufności, integralności i dostępności informacji dla upoważnionych użytkowników.

Regulacja opisuje też wytyczne w zakresie monitorowania, wykrywania i reagowania na zdarzenia dotyczące bezpieczeństwa. Wprowadza ona wymogi, które muszą zostać spełnione w zakresie złośliwego oprogramowania, aby wykrywać, blokować i reagować na ataki cybernetyczne. Określa zasady dotyczące rejestracji, klasyfikacji, oceny, komunikacji i zarządzania incydentami. Opisuje też rozwiązania z zakresu cyber intelligence, które pozwalają przewidywać i reagować na cyberzagrożenia. Poszczególne komórki organizacyjne są odpowiedzialne za raportowanie incydentów do organów decyzyjnych. Osobne procedury

dotyczą zgłaszania sytuacji nadzwyczajnych oraz zgłaszania incydentów organom nadzorczym i do Krajowego Systemu Cyberbezpieczeństwa.

Dokument określa też zasady, których muszą przestrzegać zewnętrzni dostawcy. M.in. opisuje kryteria certyfikacji usług świadczonych przez dostawców na podstawie ich poziomu ryzyka cyberbezpieczeństwa. Określa też działania w zakresie monitoringu i kontroli cyberryzyka związanego ze świadczeniem usług przez strony trzecie w okresie trwania umowy.

Osobne zasady dotyczą realizacji regularnych testów dotyczących identyfikacji, zarządzania i eliminacji podatności w celu zapobiegania atakom i incydentom naruszającym cyberbezpieczeństwo. Polityka odnosi się również do planów ciągłości działania (BCP) oraz planów odtworzenia po awarii (DRP).

Polityka wskazuje role i odpowiedzialności w zakresie zarządzania cyberbezpieczeństwem, z uwzględnieniem raportowania zarządczego. Ponadto polityka określa częstotliwość audytów prowadzonych przez wyspecjalizowane podmioty zewnętrzne. Częstotliwość wynika m.in. z wymagań regulacyjnych (w tym z Ustawy o krajowym systemie cyberbezpieczeństwa), a także w odniesieniu do uznanych standardów i norm branżowych, takich jak ISO/IEC 27001 czy PCI DSS.

Najwyższy szczebel zarządzania, który odpowiada za politykę

Za opracowanie i aktualizację polityki odpowiada Chief Information Security Officer (CISO), który raportuje bezpośrednio do wiceprezesa Zarządu kierującego Pionem Transformacji Cyfrowej. Kwestie związane z cyberbezpieczeństwem regularnie omawia też właściwy komitet ds. zarządzania ryzykiem operacyjnym, któremu przewodniczy wiceprezes Zarządu kierujący Pionem Zarządzania Ryzykiem, a zastępuje go członek Zarządu kierujący Pionem Prawnym i Zgodności.

Stosowanie w spółkach zależnych Banku

Polityka obowiązuje w Grupie Kapitałowej.