ROLA SYSTEMÓW KONTROLI DOSTĘPU

Andrzej Mendak
UNICARD SA

Systemy kontroli dostępu (KD) to często integralna część polityki bezpieczeństwa w firmach. Pomagają w jej egzekwowaniu i stanowią istotną składową systemu bezpieczeństwa. Celem SKD jest precyzyjne zarządzanie uprawnieniami użytkowników, aby dostęp do zasobów oraz informacji był ograniczony do odpowiednich osób. Dają możliwość śledzenia i rejestrowania zdarzeń, co jest ważne dla wykrywania nieprawidłowości i przeprowadzania dochodzeń po incydentach.

Aby system realnie wspierał procedury bezpieczeństwa, musi zostać dopasowany do potrzeb firmy. W artykule wyjaśnię, jak wykorzystać kontrolę dostępu, tworząc politykę ochrony dla organizacji.

AUDYT POTRZEB ORGANIZACJI

Nie ma jednego idealnego systemu kontroli dostępu dla wszystkich firm. Każda organizacja ma indywidualne potrzeby, mierzy się z innymi wyzwaniami.
Aby dobrać odpowiednie zabezpieczenia, warto przeprowadzić audyt, który zawiera m.in.:

- analizę obecnych praktyk w kontekście kontroli dostępu;
- identyfikację kluczowych zasobów;
- oceny ryzyka w sytuacji nieautoryzowanego dostępu;
- analizę potrzeb użytkowników;
- identyfikację norm i przepisów, które musi spełniać system KD.

ANALIZA OBECNYCH PRAKTYK I POLITYKI BEZPIECZEŃSTWA

Pierwszym krokiem jest dokładne przeanalizowanie istniejących procedur bezpieczeństwa. W tym celu należy szczegółowo przejrzeć wszystkie procesy, narzędzia i stosowane w firmie praktyki.

W trakcie audytu szczególną uwagę trzeba zwrócić na słabości, luki lub potencjalne zagrożenia w obecnych praktykach. Obejmuje to zarówno zagrożenia zewnętrzne, jak i wewnętrzne, a także możliwości nadużyć lub niezamierzonego naruszenia procedur.

IDENTYFIKACJA KLUCZOWYCH ZASOBÓW I OBSZARÓW DO OCHRONY

Kolejnym krokiem jest stworzenie kompleksowego spisu zasobów organizacji, któ-

re wymagają ochrony. Obejmuje to np. pomieszczenia, w których przechowywane są ważne dokumenty, sprzęt komputerowy, oprogramowanie, także magazyny czy serwerownie.

Po zidentyfikowaniu zasobów, ważne jest ich sklasyfikowanie według poziomu wrażliwości i znaczenia dla działalności organizacji. Niektóre dane, takie jak informacje osobowe klientów czy tajne dokumenty korporacyjne, mogą wymagać wyższego poziomu ochrony. System kontroli dostępu wspomaga ten proces poprzez fizyczne zabezpieczenie pomieszczeń, gdzie znajdują się wrażliwe dane.

Na podstawie oceny ryzyka i znaczenia poszczególnych zasobów należy ustalić priorytety w zakresie ich ochrony. Zasoby o największym znaczeniu i najwyższym ryzyku powinny być chronione w pierwszej kolejności lub wymagać szczególnej kontroli dostępu, np. weryfikacji dwuskładnikowej.

OCENA RYZYKA W RAZIE NIEAUTORYZOWANEGO DOSTĘPU

Aby dobrać odpowiedni system, ważne jest zrozumienie, jakie mogą być konsekwencje nieautoryzowanego dostępu lub innych naruszeń bezpieczeństwa. Należy rozważyć potencjalne straty finansowe, uszczerbek na reputacji, przerwy w działalności firmy, a także konsekwencje prawne.

ANALIZA POTRZEB RÓŻNYCH GRUP UŻYTKOWNIKÓW

Ważna jest też identyfikacja różnych grup użytkowników - pracowników, jak i gości, którzy odwiedzają firmę (kontrahenci, dostawcy czy kandydaci do rekrutacji) oraz zrozumienie ich ról w organizacji.

Konieczne jest zebranie informacji o uprawnieniach ich dostępu i wymaganiach dotyczących bezpieczeństwa. Należy przemyśleć, kiedy i w jaki sposób poszczególne grupy użytkowników będą korzystać z systemów kontroli dostępu.

ZGODNOŚĆ SYSTEMU Z PRZEPISAMI OBOWIĄZUJĄCEGO PRAWA CZY O OCHRONIE DANYCH OSOBOWYCH

Szczególnie dotyczy to instytucji o wysokim stopniu odpowiedzialności za dane osobowe, takich jak szpitale, kancelarie, urzędy czy banki.

Przykładem jest RODO (znane także jako GDPR), które jest rozporządzeniem o ochronie danych w Unii Europejskiej. Każdy system KD wdrażany w firmach działających na terenie UE musi spełniać rygorystyczne wymogi RODO. Obejmuje to odpowiednie mechanizmy bezpieczeństwa, takie jak szyfrowanie oraz umożliwienie użytkownikom dostępu do ich danych i kontrolę nad nimi.

Z kolei lokalne przepisy mogą narzucać instytucjom wymogi dotyczące przejść ewakuacyjnych, odbywania regularnych audytów bezpieczeństwa czy sposobów reagowania na incydenty.

DOBÓR SYSTEMU DLA POTRZEB FIRMY

Dobrze przeprowadzony audyt jest podstawą wyboru systemu KD, który będzie spełniał specyficzne wymogi firmy i odpowiadał na indywidualne wyzwania w kwestii bezpieczeństwa.

SYSTEM LOKALNY CZY OPARTY NA CHMURZE

W sektorze bezpieczeństwa fizycznego obserwujemy istotną ewolucję. Tradycyjne rozwiązania kontroli dostępu oparte o serwery lokalne ustępują miejsca systemom bazującym na technologii chmury (ACaaS, czyli Access Control as a Service), takim jak impero 360 od UNICARD Systems.

Główne korzyści tego systemu chmurowego to:

- wgląd do systemu możliwy jest za pomocą dowolnego urządzenia z dostępem do Internetu i przeglądarki, co umożliwia logowanie się z każdego zakątka świata;
- implementacja rozwiązania chmurowego eliminuje potrzebę inwestycji w serwer, specjalistyczny sprzęt IT czy zatrudniania ekspertów IT, co obniża koszty początkowe;
- zarządzanie bezpieczeństwem i regularne aktualizacje są w pełni obsługiwane przez Data

Center, eliminując potrzebę ciągłej, samodzielnej interwencji wymaganej w przypadku serwerów lokalnych;
- systemy ACaaS wyróżniają się zdolnością do adaptacji oraz łatwej rozbudowy, co pozwala na dopasowanie ich do ewoluujących potrzeb organizacji;
- model płatności abonamentowej pozwala rozłożyć wydatki w czasie (często są to płatności miesięczne lub roczne), dzięki czemu nawet firmy z ograniczonym budżetem mogą korzystać z tej technologii;
- dzięki integracji z Azure Active Directory, z jednego konta możliwe jest zarządzanie tożsamościami użytkowników w systemach KD i IT. To nie tylko ułatwia pracę, ale przede wszystkim pomaga w utrzymaniu bezpieczeństwa.

DOBÓR ZABEZPIECZEŃ

W doborze zabezpieczeń ważne jest zwrócenie uwagi na zaawansowane technologie, takie jak:

- dostęp mobilny, czyli wykorzystanie smartfonów zamiast kart dostępu;
- uwierzytelnianie wielopoziomowe, np. indywidualny identyfikator + PIN dla miejsc szczególnie chronionych;
- biometria, np. autoryzacja za pomocą odcisku palców, skanu twarzy czy tęczówki.

Oprócz tego firmy mogą zastosować dodatkowe środki ochrony: monitoring wizyjny, system SSWiN, kołowroty, czy bramki.

INTEGRACJA Z INNYMI SYSTEMAMI

Aby zoptymalizować zarządzanie i podnieść poziom bezpie-

czeństwa, systemy kontroli dostępu powinny mieć możliwość efektywnej integracji z obecnymi lub planowanymi rozwiązaniami, jak system monitoringu wizyjnego CCTV, system alarmowe SSWiN czy system PPOŻ.

Elastyczny system dostępowy powinien bez trudu współpracować także z:

- systemami parkingowymi, rezerwacją sal konferencyjnych czy awizacją gości (VMS);
- systemami zarządzania budynkiem BMS, w tym kontrolą wind, ogrzewania, oświetlenia, klimatyzacji oraz czujnikami dymu;
- systemami do rejestracji czasu pracy;
- urządzeniami higieny produkcji;
- systemami ERP, takimi jak: SAP, Enova, Sage Symfonia, TETA, Comarch ERP Optima.

USTALENIE ZASAD ZARZĄDZANIA SYSTEMEM KONTROLI DOSTĘPU

Podstawą tego etapu jest opracowanie zasad dostępu do poszczególnych zasobów w firmie i przydzielenie odpowiednich uprawnień. Uprawnienia mogą być nadawane indywidualnie oraz dla grup pracowników, np. różne dla osób zatrudnionych na produkcji, magazynie czy w kadrach.

Uprawnienia można też rozróżniać ze względu na:

- dni tygodnia;
- godziny;
- lokalizacje, gdy system jest rozproszony;
- wykonywane zadania;
- zmiany nocne/dzienne;
- poziomy certyfikacji i kwalifikacji.

Zarządzanie systemem kontroli dostępu wymaga także gotowości na nietypowe i krytyczne sytuacje. Aby SKD realnie wspierał politykę bezpieczeństwa organizacji, należy opracować scenariusze reakcji w przypadku wykrycia nieautoryzowanego dostępu, prób włamania, czy innych naruszeń i zdarzeń w systemie.

W sytuacji zagrożenia bezpieczeństwa niezwykle ważne jest posiadanie jasno określonych procedur, np. ewakuacji.

SZKOLENIA PERSONELU

Głównym zadaniem szkolenia jest upewnienie się, że każdy pracownik zna cel wdrożenia kontroli dostępu oraz rozumie, w jaki sposób system przyczynia się do ochrony pracowników i zasobów firmy.

Pracownicy muszą też wiedzieć, jak postępować w przypadku awarii systemu, zagubienia lub uszkodzenia karty dostępu, a także jak reagować na potencjalne naruszenia bezpieczeństwa. Kluczowa jest też świadomość konsekwencji związanych z niewłaściwym użyciem identyfikatorów lub dzieleniem się nimi z innymi osobami.

Szkolenia można dostosować też do różnych ról i poziomów dostępu w organizacji. Na przykład, personel ochrony może potrzebować bardziej zaawansowanego wdrożenia, podczas gdy pracownicy biurowi zwykle potrzebują podstawowych informacji na temat codziennego użytkowania SKD.

MONITORING I OCENA PRACY SYSTEMU

System kontroli dostępu powinien być regularnie monitorowany i oceniany pod kątem efektywności i skuteczności działania.

Ocena powinna obejmować testowanie niezawodności komponentów systemu, analizę zdarzeń, a także przegląd zgodności z przepisami prawa oraz aktualną polityką bezpieczeństwa. Regularne przeglądy poprawności działania systemu oraz jego konserwacja są zalecane przez producentów SKD, a monitoring zwykle można przeprowadzić we współpracy z dostawcą systemu.

Te działania pozwalają na utrzymanie systemu w prawidłowym stanie technicznym oraz dostosowanie go do ewoluujących potrzeb i wyzwań polityki bezpieczeństwa.

PODSUMOWANIE

Dobrze opracowana – a przede wszystkim skutecznie wdrożona – polityka bezpieczeństwa to nie tylko ochrona przed zagrożeniami cybernetycznymi, ale również efektywne zabezpieczenia fizyczne.

Systemy kontroli dostępu są kluczowym elementem strategii bezpieczeństwa, chroniąc sprzęt, dokumenty oraz dając poczucie bezpieczeństwa pracownikom. Ważne jest nie tylko dobrze dopasowane rozwiązanie, ale też wypracowanie procedur oraz szkolenie osób, które z systemu będą korzystać.

Cały proces – od audytu potrzeb, po monitoring i ocenę pracy SKD – pozwala zadbać, aby ochrona fizyczna w budynku była dostosowana do specyficznych wymagań i ryzyk, które niesie ze sobą działalność danej organizacji.