

2. Fizyczne bezpieczeństwo urządzeń – ochrona zaczyna się od klucza, szuflady i plecaka



W jednej z firm produkcyjnych do biura wszedł nieznany mężczyzna. Pracownicy uznali, że to ktoś z firmy, więc nikt nie zareagował. Dopiero po godzinie zauważono brak służbowego laptopa. Monitoring nie pozwolił ustalić tożsamości sprawcy.

Choć dużo uwagi poświęca się dziś cyberbezpieczeństwu, wiele incydentów zaczyna się od prostego, fizycznego dostępu do urządzenia. Wystarczy chwila nieuwagi – niezabezpieczony laptop czy brak kontroli wejść do biura – by doszło do poważnego incydentu bezpieczeństwa związanego z danymi.

Ryzyka związane z bezpieczeństwem urządzeń biurowych

W codziennym rytmie pracy biuro wydaje się przestrzenią bezpieczną i przewidywalną. Tymczasem to właśnie tutaj może dochodzić do zdarzeń, które potrafią sparaliżować organizację – często w sposób zaskakująco prosty. Wystarczy moment nieuwagi, niedopilnowana procedura albo błędne założenie, że „w naszej firmie to niemożliwe”. Oto przykłady:

Nieautoryzowany dostęp do pomieszczeń, kradzież sprzętu

Brak kontroli nad dostępem do biura to jedno z poważniejszych zagrożeń dla bezpieczeństwa fizycznego urządzeń. Otwarte pomieszczenia po godzinach pracy, współdzielone karty dostępu czy niekontrolowany ruch gości i podwykonawców – to wszystko zwiększa ryzyko, że osoba nieuprawniona uzyska dostęp do sprzętu lub dokumentów. Wystarczy krótka obecność przy komputerze, żeby skopiować dane lub zainfekować system złośliwym oprogramowaniem za pomocą nieautoryzowanego nośnika.

Równie niebezpieczna jest kradzież sprzętu. Laptopy, telefony, dyski zewnętrzne czy pendrive'y to dziś podstawowe narzędzia pracy. Nie należy pozostawiać ich bez nadzoru w ogólnodostępnych pomieszczeniach. W przypadku dłuższej nieobecności urządzenia należy schować w zamykanej szafce. Podczas podróży i w przestrzeniach publicznych zaleca się korzystanie z linek zabezpieczających, które utrudniają kradzież laptopa. Dodatkowe nośniki, takie jak dyski zewnętrzne czy pendrive'y, zawsze powinny być przechowywane w bezpiecznym miejscu.

Niewłaściwe zabezpieczenie serwerowni i infrastruktury IT

Konsekwencje tych zaniedbań mogą prowadzić do manipulacji sprzętem, awarii lub celowego zakłócenia działania systemów. Obszary te powinny być objęte kontrolą dostępu, z rejestracją wejść i ograniczeniem uprawnień. Brak nadzoru w postaci monitoringu wizyjnego czy plomb na obudowach urządzeń zwiększa ryzyko nieautoryzowanych działań.



Zagrożenia środowiskowe

Pożary, zalania czy awarie zasilania bądź klimatyzacji, mogą prowadzić do utraty danych i uszkodzenia sprzętu. Odpowiednie zabezpieczenia – czujniki (m.in. kontrola temperatury, wilgotności, zadymienia), systemy awaryjnego zasilania oraz procedury reagowania – powinny być traktowane jako integralna część systemu bezpieczeństwa informacji.

Sprzęt służbowy poza firmą

Praca zdalna i podróże służbowe stały się codziennością. To ogromna wygoda, ale też wyzwanie dla bezpieczeństwa informacji. Laptop czy telefon służbowy, który opuszcza firmę, przestaje być chroniony murami biura, alarmem i systemem kontroli dostępu. Od tej chwili wszystko zależy od użytkownika – jego ostrożności, świadomości i przestrzegania zasad.

Każda organizacja powinna opracować własne procedury korzystania ze sprzętu poza siedzibą, dostosowane do specyfiki działalności, rodzaju przetwarzanych danych i poziomu ryzyka. Wśród dobrych praktyk, powszechnie stosowanych w firmach dbających o bezpieczeństwo informacji, można wyróżnić kilka kluczowych zasad.

Korzystanie ze sprzętu poza biurem

Sprzęt służbowy nie powinien „wędrować” bez konkretnego celu. Jego użycie poza siedzibą firmy powinno wynikać z obowiązków służbowych – np. pracy w terenie czy spotkania z klientem. Każde wyniesienie urządzenia należy zatwierdzić i odnotować w rejestrze aktywów, tak aby było jasne, kto odpowiada za sprzęt i gdzie on się aktualnie znajduje.

Zasady bezpieczeństwa dotyczą także pracy zdalnej. Jeśli w mieszkaniu przebywają inni użytkownicy – domownicy, goście czy serwisanci – każdorazowe zablokowanie ekranu po odejściu od urządzenia wciąż powinno być nawykiem. Pamiętajmy, że sprzęt służbowy jest przeznaczony wyłącznie do realizacji obowiązków zawodowych, nie należy go udostępniać innym osobom. Jeden błąd może skutkować utratą danych i zagrożeniem bezpieczeństwa firmy.

Dobre praktyki bezpieczeństwa poza siedzibą

Najważniejsza zasada: **sprzęt zawsze musi pozostać pod kontrolą użytkownika.**

Wystarczy moment nieuwagi, by laptop zniknął z tylnego siedzenia samochodu, a telefon został w kawiarni razem z poranną kawą. Pozostawienie urządzenia w bagażniku samochodu, na lotnisku czy w sali konferencyjnej to otwarte zaproszenie dla niepowołanych osób.

Ryzyko wzrasta, gdy sprzęt przenoszony jest w torbie z firmowym logo – to czytelny sygnał, że wewnątrz mogą znajdować się wartościowe dane. W sytuacjach wymagających pracy w przestrzeni publicznej warto stosować filtry prywatyzujące, które skutecznie ograniczają możliwość podejrzenia ekranu przez osoby postronne.

Utrata lub kradzież sprzętu? Liczy się szybka reakcja!

Zagubienie lub utrata służbowego urządzenia w wyniku kradzieży to stresujące sytuacje. Dobrze przygotowana procedura pozwala działać sprawnie, szybko i bez chaosu. Każda minuta zwłoki zwiększa ryzyko nieautoryzowanego dostępu, dlatego incydent należy zgłosić niezwłocznie.



Tak jak w przypadku korzystania ze sprzętu poza biurem, również tutaj warto mieć jasne zasady postępowania. Poniższe wskazówki opierają się na sprawdzonych praktykach stosowanych w organizacjach dbających o bezpieczeństwo informacji.

Co robić?

- **Zgłoszenie** – należy niezwłocznie poinformować przełożonego oraz zespół IT lub bezpieczeństwa informacji. Najlepiej zrobić to telefonicznie, a potem potwierdzić e-mailem na dedykowany adres.
- **Dane** – w zgłoszeniu warto podać swoje dane, rodzaj urządzenia oraz opisać okoliczności zdarzenia: gdzie i kiedy doszło do utraty.
- **Reakcja** – zespół lub osoba odpowiedzialna za bezpieczeństwo w firmie ocenia ryzyko naruszenia danych i podejmuje działania, np. zdalna blokada lub usunięcie danych z urządzenia, zgłoszenie sprawy właściwym organom (np. Policja, Straż Graniczna)
- **Analiza** – incydent powinien zostać przeanalizowany pod kątem ewentualnego zgłoszenia do organu nadzorczego.
- **Ewidencja i wnioski** – zdarzenie należy odnotować w rejestrze incydentów, a na podstawie analizy wyciągnąć wnioski, które pomogą usprawnić procedury i ograniczyć ryzyko w przyszłości.

Jasne zasady i sprawna komunikacja z zespołem IT to fundament skutecznego działania w sytuacji kryzysowej.

Zdalne zarządzanie – niewidzialne tarcze bezpieczeństwa

Sprzęt służbowy towarzyszy pracownikom w podróży, w domu, na spotkaniach – często poza zasięgiem bezpośredniego wsparcia IT. W takich warunkach kluczowe stają się rozwiązania umożliwiające zdalne zarządzanie urządzeniami i szybkie reagowanie na potencjalne zagrożenia, zanim drobny incydent przerodzi się w poważny wyciek danych.

Dwa najważniejsze narzędzia w tym obszarze to MDM (Mobile Device Management) i EDR (Endpoint Detection and Response). Choć różnią się zakresem działania, łączy je wspólny cel – utrzymanie kontroli nad sprzętem i danymi, niezależnie od miejsca, w którym się znajdują.

MDM – zarządzanie urządzeniami mobilnymi

Systemy MDM umożliwiają zdalne zarządzanie telefonami, tabletami i laptopami należącymi do organizacji. Dzięki nim można wymuszać stosowanie zabezpieczeń, takich jak: szyfrowanie, silne hasła czy aktualizacje, kontrolować instalację aplikacji i dostęp do zasobów firmowych, a także oddzielać dane służbowe od prywatnych na urządzeniach pracowników. W przypadku utraty sprzętu możliwe jest jego zablokowanie lub zdalne usunięcie danych. Z perspektywy użytkownika, MDM działa zazwyczaj w tle, niezauważalnie — dla organizacji to kluczowe narzędzie, które pozwala utrzymać spójny poziom bezpieczeństwa, nawet w środowisku rozproszonym, w przypadku pracy zdalnej czy hybrydowej.



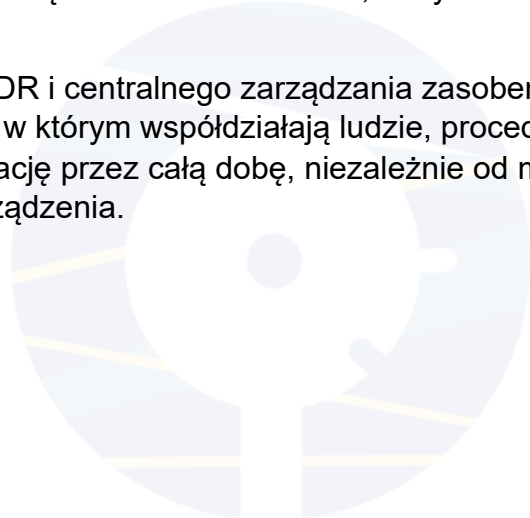
EDR – inteligentna ochrona punktów końcowych

EDR to system, który monitoruje aktywność urządzeń i reaguje na zagrożenia w czasie rzeczywistym. Działa jak cyfrowy strażnik – analizuje zachowanie systemu, aplikacji i użytkownika, wychwytyjąc podejrzane wzorce. W razie wykrycia nieprawidłowości może zablokować proces, odłączyć urządzenie od sieci lub powiadomić administratora. W praktyce pozwala szybko reagować na incydenty, próby kradzieży danych czy nieautoryzowane zmiany w konfiguracji.

Pełna kontrola nad zasobem urządzeń firmowych

Nowoczesne podejście do bezpieczeństwa informacji wykracza poza ochronę pojedynczego laptopa – obejmuje zarządzanie całym zasobem sprzętu: od komputerów i smartfonów po urządzenia peryferyjne. Dzięki centralnym systemom nadzoru dział bezpieczeństwa ma pełen wgląd w lokalizację, stan techniczny i poziom zabezpieczeń każdego urządzenia. Automatyczne aktualizacje, kontrola konfiguracji czy blokowanie nieautoryzowanych urządzeń to dziś standard, który realnie ogranicza ryzyko wystąpienia incydentów.

Połączenie MDM, EDR i centralnego zarządzania zasobem urządzeń tworzy spójny ekosystem ochrony, w którym współdziałają ludzie, procedury i technologie. To tarcza, która chroni organizację przez całą dobę, niezależnie od miejsca, w którym znajdują się użytkownicy i ich urządzenia.



EUROPEJSKI

MIESIĄC

CYBER

BEZPIECZEŃSTWA



2 z 12

Fizyczne bezpieczeństwo urządzeń. Najważniejsze zasady

- Zawsze zabezpieczaj sprzęt – zamykane biurko, sejf czy linka antykradzieżowa. Proste środki – konkretna ochrona.
- Laptop i telefon trzymaj pod ręką – zostawiony bez nadzoru, nawet na minutę, przestaje być bezpieczny.
- Chroń dane od momentu uruchomienia urządzenia – silne hasła, automatyczna blokada ekranu, filtry prywatyzujące, szyfrowanie. Zero kompromisów.
- Bądź dyskretny podczas pracy w terenie – żadnych firmowych oznaczeń, ekran zabezpieczony filtrem, sprzęt pod kontrolą.
- Technologia wspiera Twoje bezpieczeństwo – MDM i EDR pozwalają reagować zdalnie i utrzymać kontrolę.
- Incydenty zgłaszaj od razu – szybka reakcja zgodna z procedurą – to szansa na ograniczenie negatywnych skutków.
- Poważnie traktuj szkolenia – wiedza zespołu to realna tarcza ochronna.
- Z każdego zdarzenia wyciągaj lekcję – analiza incydentów wzmacnia system i buduje kulturę bezpieczeństwa.



Pytania kontrolne:



Czy dostęp do biura i pomieszczeń technicznych jest kontrolowany, a osoby z zewnątrz rejestrowane?



Czy laptopy, telefony i nośniki danych nie są pozostawiane bez nadzoru w ogólnodostępnych miejscach?



Czy pracownicy blokują ekran komputera po odejściu od stanowiska pracy?



Czy urządzenia są przechowywane w zamykanych szafkach lub biurkach podczas dłuższej nieobecności?



Czy wnoszenie sprzętu poza firmę jest uzasadnione i odnotowane w ewidencji?



Czy pracownicy wiedzą, jak postępować w przypadku utraty lub kradzieży urządzenia?



Czy firma ma możliwość zdalnego zablokowania lub usunięcia danych z utraconego sprzętu?



Czy urządzenia firmowe są objęte centralnym zarządzaniem (np. MDM, EDR)?