

1. Inwentaryzacja i zarządzanie sprzętem – pierwszy krok do bezpieczeństwa



W małej firmie usługowej pracownik działu obsługi klienta po 3 miesiącach odszedł z dnia na dzień z pracy. Po kilku dniach menedżer zauważył, że do klientów wciąż wysyłane są wiadomości SMS z przydzielonego mu numeru służbowego. Co gorsza, treść tych wiadomości sugerowała, że były pracownik oferuje konkurencyjne usługi, wykorzystując dane kontaktowe klientów firmy.

Jak się okazało, nikt nie spisał protokołu przekazania sprzętu, a telefon nie był zabezpieczony ani firmowym profilem, ani systemem MDM. Urządzenia nie było w żadnym rejestrze, a firma nie potrafiła ustalić, ile takich telefonów posiadają obecni i byli pracownicy. Brak ewidencji i procedury zwrotu spowodował nie tylko utratę sprzętu, ale i ryzyko wycieku danych oraz naruszenia dobrego imienia firmy.

Bezpieczeństwo zaczyna się od wiedzy o zasobach IT

Zapewnienie w firmie bezpieczeństwa urządzeń oraz związanego z nimi oprogramowania nie zaczyna się od budowania złożonych systemów, lecz od wiedzy o tym, co faktycznie znajduje się w zasobach organizacji. Wiele zagrożeń w obszarze zarządzania sprzętem i oprogramowaniem wynika z chaosu organizacyjnego. Firmy często nie wiedzą:

- ile urządzeń znajduje się w zasobach i jakiego są typu,
- kto korzysta z konkretnego sprzętu oraz kto jest za niego odpowiedzialny,
- kiedy dany komputer został przekazany użytkownikowi i czy został zwrócony,
- który laptop był aktualizowany, a z którego od lat nikt nie korzystał,
- co stało się z pendrive'em, który „zawsze leżał w szufladzie”,
- jakie oprogramowanie jest zainstalowane na urządzeniach oraz kiedy przeprowadzono ostatnią aktualizację.

Taki brak kontroli otwiera drzwi nie tylko do strat finansowych, ale również do naruszeń bezpieczeństwa danych, konsekwencji prawnych czy utraty zaufania klientów.

Dlaczego nieewidencjonowany sprzęt stanowi zagrożenie?

Nieewidencjonowany laptop czy telefon to nie tylko problem logistyczny – to potencjalna luka bezpieczeństwa. Takie urządzenie może zawierać dane firmowe, nieaktualne, podatne na cyberataki oprogramowanie czy dostęp do sieci firmowej. Brak protokołu przekazania oznacza, że nie wiadomo, kto i od kiedy odpowiada za jego stan. Brak oznakowania urządzenia utrudnia audyt, a nawet odzyskanie sprzętu po zakończeniu współpracy.



Inwentaryzacja a ochrona danych i RODO

Z perspektywy zgodności z przepisami (np. RODO), firma powinna wiedzieć, przez kogo i w jakim celu są przetwarzane dane osobowe klientów. Nie można skutecznie chronić danych, jeśli nie wiadomo, na jakich urządzeniach się znajdują.

Dlatego tak ważna jest regularna inwentaryzacja i zarządzanie sprzętem w firmie. Nie może to być sytuacja jednorazowa. To proces obejmujący ewidencję, monitorowanie i kontrolę wszystkich zasobów IT, od komputerów i telefonów, przez zgodne z polityką firmy oprogramowanie, aż po urządzenia biurowe. Kluczowe etapy to: sporządzenie szczegółowej listy tych zasobów (inwentaryzacja), śledzenie ich stanu, lokalizacji i użytkowania (monitorowanie), dbanie o ich sprawność (serwisowanie) oraz przygotowywanie przyszłych działań (planowanie). Proces ten pozwala obniżyć koszty, zwiększyć bezpieczeństwo, podnieść poziom odpowiedzialność pracowników i spełnić wymogi prawne.

Ewidencja, protokoły, oznakowanie sprzętu i oprogramowania

Identyfikacja

Pierwszym krokiem do skutecznego zarządzania infrastrukturą techniczną firmy jest dokładna **identyfikacja wszystkich** wykorzystywanych **urządzeń i oprogramowania**. Sprzęt firmowy to nie tylko komputery i telefony, ale również routery, punkty dostępowe Wi-Fi, drukarki, skanery, urządzenia wielofunkcyjne, rejestratory, tablety, dyski zewnętrzne, pendrive'y, a w wielu branżach także specjalistyczne urządzenia podłączane do sieci, takie jak kamery czy czujniki. Dobrym rozwiązaniem jest tworzenie przejrzystej klasyfikacji sprzętu, np. według kategorii: komputery, urządzenia mobilne, pamięci przenośne, drukarki oraz urządzenia prywatne używane do celów służbowych (BYOD – Bring Your Own Device). Taki podział pozwala określić odpowiednie zasady ochrony, kontroli i nadzoru dla każdej grupy urządzeń. W realiach pracy hybrydowej oraz rosnącej popularności modelu BYOD lista ta powinna obejmować również prywatny sprzęt pracowników wykorzystywany w ramach obowiązków służbowych.

Ewidencja

Następnym elementem jest **ewidencja urządzeń i oprogramowania** – systematyczna i stale aktualizowana baza danych, w której zapisujemy wszystkie informacje o sprzęcie i oprogramowaniu, m.in.: nazwę, model, numer seryjny, datę zakupu, przeglądu, lokalizację, osobę odpowiedzialną. Dobrze prowadzona ewidencja pozwala szybko zidentyfikować, które urządzenia są aktywne, które przeszły już na „emeryturę” i które mogą stanowić potencjalne ryzyko. Rejestr taki można prowadzić w formie prostej tabeli w arkuszu kalkulacyjnym, ale wraz ze wzrostem skali warto sięgnąć po specjalistyczne rozwiązania ITAM (IT Asset Management), które pozwalają także na monitorowanie stanu technicznego, gwarancji, podatności czy przypisanych użytkowników. Aktualna ewidencja wspiera zarządzanie majątkiem i pozwala na szybkie reagowanie na incydenty. Dodatkową wartością – w kontekście bezpieczeństwa firmy – może być integracja rozwiązań ITAM z systemem SIEM (Security Information and Event Management) służącym do monitorowania i analizy zdarzeń w czasie rzeczywistym.



Przekazanie

Integralną częścią ewidencji sprzętu powinien być **protokół przekazania urządzenia pracownikowi**. Każdy telefon, laptop czy inne urządzenie powinno zostać formalnie przypisane do konkretnej osoby, wraz z datą, stanem technicznym, wykazem akcesoriów i potwierdzeniem odbioru. Taki dokument nie tylko zabezpiecza firmę w razie uszkodzenia lub zgubienia sprzętu, ale także wzmacnia poczucie odpowiedzialności użytkownika. Protokół może mieć formę papierową lub elektroniczną, ważne jednak, by był częścią obowiązującej procedury wdrażania nowego pracownika lub zmiany stanowiska.

Oznakowanie

Ostatnim, lecz równie istotnym elementem zarządzania sprzętem jest **fizyczne oznakowanie urządzeń**. Ułatwia to identyfikację i inwentaryzację sprzętu firmowego. W praktyce oznacza to, że każdy egzemplarz sprzętu firmowego powinien posiadać unikalny identyfikator – numer lub naklejkę z kodem kreskowym, tagiem RFID lub kodem QR. Dzięki temu możliwa jest szybka identyfikacja i przypisanie urządzenia do konkretnej pozycji w rejestrze. Oznaczenia powinny być trwałe, trudne do usunięcia i jednoznaczne. Coraz popularniejsze są systemy inwentaryzacji mobilnej, w których wystarczy zeskanować kod QR telefonem, by wyświetlić historię urządzenia, informacje o serwisowaniu czy dane przypisanego użytkownika.

Wszystkie te elementy – lista sprzętu, rejestr, protokoły i oznaczenia – tworzą wspólnie ramy zarządzania zasobami IT, które mają nie tylko znaczenie porządkowe, ale bezpośrednio wpływają na bezpieczeństwo organizacji i powinny być zawarte w **polityce bezpieczeństwa firmy**, wdrożonej i regularnie aktualizowanej.

Dobrze zorganizowany system zarządzania sprzętem to inwestycja w bezpieczeństwo i efektywność.

EUROPEJSKI

MIESIĄC

CYBER

BEZPIECZEŃSTWA



Inwentaryzacja i zarządzanie sprzętem i oprogramowaniem

Najważniejsze zasady

- Sporządź kompletną listę urządzeń i oprogramowania w firmie.
- Prowadź ewidencję – cyfrową lub papierową i na bieżąco ją aktualizuj.
- Wydawaj sprzęt i/lub oprogramowanie pracownikom za potwierdzeniem odbioru.
- Oznaczaj urządzenia unikalnymi numerami lub kodami.
- Zintegruj zarządzanie sprzętem i oprogramowaniem z polityką bezpieczeństwa IT.

☒ ☐ Pytania kontrolne

- ☐ ☐ Czy została przygotowana pełna lista wszystkich urządzeń w firmie (IT i biurowych)?
- ☐ ☐ Czy prowadzona jest centralna ewidencja sprzętu i oprogramowania?
- ☐ ☐ Czy opracowano wzór protokołu przekazania sprzętu/oprogramowania pracownikowi?
- ☐ ☐ Czy każde urządzenie zostało oznakowane w sposób unikalny (np. kody QR, RFID, naklejki)?
- ☐ ☐ Czy wdrożono procedurę okresowej kontroli poprawności i kompletności danych w ewidencji (np. spis z natury)?
- ☐ ☐ Czy raportowany jest sprzęt zaginiony, uszkodzony lub bez wsparcia producenta?
- ☐ ☐ Czy zarządzanie sprzętem zostało zintegrowane z polityką bezpieczeństwa firmy?
- ☐ ☐ Czy zagadnienia związane z zarządzaniem sprzętem uwzględniono w szkoleniach pracowników na każdym etapie ich kariery?