

4. Bezpieczne korzystanie z telefonów służbowych



Tłok w autobusie. Złodziej sięga do kieszeni jednego z pasażerów i wyjmując niespostrzeżenie jego telefon. Brak blokady ekranu sprawia, że w kilka sekund uzyskuje dostęp do całej zawartości – służbowe maile, dane klientów, dokumenty. Instaluje oprogramowanie szpiegujące, a następnie oddaje urządzenie do biura rzeczy znalezionych. Firma i pracownik cieszą się, że telefon został odzyskany. Nie wiedzą jednak, że od tej chwili każda czynność wykonana na tym urządzeniu jest monitorowana przez cyberprzestępców, a ważne firmowe dane trafiają na ich serwery. Jak uniknąć takiego scenariusza?

Urządzenia mobilne w firmach z rozbudowaną infrastrukturą

W firmach z rozbudowaną infrastrukturą technologiczną bezpieczeństwo urządzeń mobilnych opiera się na sprawdzonych rozwiązaniach technologicznych. Systemy takie jak MDM (Mobile Device Management) czy EDR (Endpoint Detection and Response) pozwalają kontrolować dostęp, wymuszać silne hasła, blokować nieautoryzowane aplikacje, a w razie potrzeby – zdalnie usunąć dane z urządzenia. Cały proces nadzoruje zespół IT, który dysponuje odpowiednimi procedurami i narzędziami, by szybko reagować i nie dopuścić do naruszenia bezpieczeństwa.

Bez działu IT? Sprawdzone sposoby na zabezpieczenie telefonów

W małych firmach podejście do ochrony urządzeń mobilnych często jest mniej uporządkowane niż w dużych organizacjach. Telefony służbowe bywają używane również prywatnie – pracownicy korzystają z nich nie tylko do obsługi poczty firmowej, ale też do robienia zdjęć, kontaktu z rodziną czy przeglądania mediów społecznościowych. Tymczasem to właśnie na tych urządzeniach przechowywane są dane o dużym znaczeniu dla bezpieczeństwa firmy: dostęp do kont służbowych, informacje o klientach, dokumenty finansowe czy poufna korespondencja.

W tym tekście skupiamy się na organizacjach, które nie dysponują rozbudowanym zapleczem technicznym ani wsparciem działu IT – a mimo to powinny zadbać o bezpieczeństwo telefonów i danych, które są w nich zapisane.

Dostęp do urządzenia – pierwsza linia obrony

Nawet najbardziej zaawansowane systemy zabezpieczeń nie zastąpią podstawowej ochrony – kontroli dostępu do urządzenia. Blokada ekranu to pierwsza bariera zabezpieczająca dane służbowe przed nieuprawnionymi osobami.

Blokada telefonu – kody i hasła

Najczęściej stosowanym zabezpieczeniem jest kod PIN lub hasło. Zasada jest prosta – długie (co najmniej 14 znakowe) i nieoczywiste hasło będzie lepsze niż 1111 lub Barbara72. Należy unikać prostych sekwencji, takich jak: „1234” czy „0000”, imiona i daty



urodzenia, czy powtarzające się (a więc znane przestępcom) wzorce odblokowania. Warto również ustawić automatyczne blokowanie ekranu po krótkim czasie bezczynności, np. 30-60 sekund. W sytuacji utraty urządzenia nawet podstawowe zabezpieczenie może zdecydować o tym, czy ktoś uzyska dostęp do skrzynki e-mail lub poufnych dokumentów.

Biometria – wygoda, która wymaga rozsądku

Odcisk palca czy rozpoznawanie twarzy ułatwiają korzystanie z telefonu, dlatego biometria jest dziś powszechna. Nie powinna jednak całkowicie zastępować innych metod zabezpieczania (np. hasła czy kodu PIN). Zaleca się, aby aplikacje o podwyższonym poziomie wrażliwości, takie jak bankowość czy menedżery haseł, wymagały dodatkowego uwierzytelnienia. W takiej sytuacji pierwszą linią zabezpieczeń pozostaje tradycyjne hasło, a biometria uzupełnia je jako tzw. drugi czynnik uwierzytelniania."

Folie prywatyzujące – dodatkowa tarcza

Często pomijanym elementem bezpieczeństwa jest ochrona przed ciekawskimi spojrzeniami. Podczas podróży służbowych, spotkań czy pracy w przestrzeniach współdzielonych ekran telefonu może ujawniać poufne informacje, takie jak: treść ważnej notatki służbowej, dane kontaktowe klienta, czy nawet wpisywany właśnie kod PIN. Folia prywatyzująca sprawia, że informacje wyświetlane są widoczne jedynie dla osoby patrzącej na wprost. To prosty a jednocześnie bardzo skuteczny środek przed podglądaniem. Jego dodatkową funkcją może być ochrona ekranu przed uszkodzeniami mechanicznymi oraz redukcja emisji niebieskiego światła, które jest szkodliwe dla oczu.

Telefon służbowy to nie prywatny gadżet

Świadomość bezpieczeństwa zaczyna się od właściwego podejścia do urządzeń mobilnych. Telefon służbowy to narzędzie pracy, a nie prywatny gadżet. Jako element infrastruktury firmy podlega tym samym zasadom ochrony co komputer czy dostęp do sieci. W praktyce jednak, szczególnie w mniejszych organizacjach, urządzenia często pełnią podwójną rolę: służą do pracy i do spraw osobistych. Choć takie rozwiązanie wydaje się wygodne, zwiększa ryzyko naruszeń bezpieczeństwa. Instalowanie gier, aplikacji rozrywkowych czy korzystanie z prywatnych kont w mediach społecznościowych może spowodować wyciek, kradzież lub utratę danych firmowych.

Aby chronić dane firmowe, należy oddzielić przestrzeń prywatną od zawodowej. Systemy Android i iOS oferują funkcję tworzenia osobnych profili lub kont użytkownika, które pozwalają oddzielić firmowe aplikacje i dane od tych prywatnych. Dzięki temu ryzyko wycieku informacji jest znacznie mniejsze. Warto pamiętać, że zagrożenie pojawia się również wtedy, gdy urządzenie trafia w ręce dziecka. Nawet krótki dostęp – „tylko jedna bajka” – może skończyć się przypadkową instalacją aplikacji lub zmianą ustawień, a w niektórych sytuacjach – nawet uzyskaniem przez cyberprzestępcę zdalnego dostępu do telefonu.

Instalowanie aplikacji – minimalizm to podstawa

Każda dodatkowa aplikacja na urządzeniu mobilnym zwiększa prawdopodobieństwo naruszenia bezpieczeństwa. Może to wynikać zarówno z podatności na błędy w oprogramowaniu, jak i z nieuczciwych praktyk polegających na wyludzaniu danych.



Dlatego warto kierować się zasadą „mniej znaczy bezpieczniej” – instaluj tylko te aplikacje, które są niezbędne do wykonywania obowiązków służbowych.

Równie istotne jest źródło instalacji. Pobieraj aplikacje wyłącznie z oficjalnych sklepów, takich jak Google Play czy App Store, które stosują mechanizmy weryfikacji i ograniczają ryzyko złośliwego oprogramowania. Kolejnym istotnym aspektem w przypadku aplikacji i oprogramowania telefonu jest ich aktualizacja. Aktualizacja nie jest kaprysem producenta, lecz mechanizmem ochrony urządzenia. Każda poprawka usuwa słabe punkty, które mogą stać się furtką dla ataków.

Kontrola uprawnień – dlaczego jest tak ważna?

Wiele aplikacji podczas instalacji żąda dostępu do funkcji, które nie są niezbędne do ich działania. Wynika to niekiedy z błędów projektowych, a czasem z zamierzonego gromadzenia danych w celach marketingowych lub analitycznych. Nieuzasadnione uprawnienia mogą prowadzić do poważnych naruszeń bezpieczeństwa.

Dostęp do kontaktów, mikrofonu, aparatu czy lokalizacji umożliwia nie tylko pozyskiwanie danych, ale również ich przesyłanie poza urządzenie – często bez wiedzy użytkownika. W środowisku służbowym, gdzie na telefonie znajdują się dane klientów, wiadomości e-mail czy dokumenty, takie sytuacje mogą skutkować utratą poufności, np. gdy aplikacja pogodowa prosi o dostęp do mikrofonu i kontaktów, a gra mobilna wymusza dostęp do lokalizacji.

Dlatego warto regularnie sprawdzać nadane aplikacjom uprawnienia i usuwać te, które są zbędne. Takie działanie pozwala zachować kontrolę nad tym, jakie dane są dostępne dla poszczególnych aplikacji. Dobrym nawykiem jest okresowe przeglądanie listy uprawnień w telefonie i weryfikacja, które aplikacje mają dostęp do mikrofonu, aparatu, lokalizacji czy kontaktów. Dzięki temu można szybko wychwycić nadmierne lub nieuzasadnione żądania, które mogą stanowić zagrożenie dla bezpieczeństwa informacji.

EUROPEJSKI
MIESIĄC
CYBER
BEZPIECZEŃSTWA



Bezpieczne korzystanie z telefonów służbowych.

Najważniejsze zasady bezpieczeństwa

Bezpieczne korzystanie z telefonów służbowych to m.in.:

- **Silne zabezpieczenia urządzenia** – aktualny system operacyjny, regularnie aktualizowane aplikacje oraz silne uwierzytelnianie (PIN, biometria).
- **Dodatkowa ochrona danych** – szyfrowanie pamięci, automatyczna blokada ekranu oraz możliwość zdalnego zablokowania lub wymazania danych w razie utraty telefonu.
- **Bezpieczna komunikacja** – korzystanie z zaufanych sieci, szyfrowanej komunikacji oraz VPN podczas pracy poza biurem.
- **Ochrona przed złośliwym oprogramowaniem** – oprogramowanie zabezpieczające oraz ostrożność przy otwieraniu e-maili, linków i załączników.
- **Szybkie zgłaszanie incydentów** – w przypadku utraty telefonu należy niezwłocznie poinformować przełożonego lub dział IT, aby umożliwić zablokowanie urządzenia i ochronę danych.



Pytania kontrolne



Czy masz ustawiony silny kod PIN lub hasło (inne niż „1234”, „Adam1993”)?



Czy ekran blokuje się automatycznie po maks. 60 sekundach bezczynności?



Czy masz folię prywatyzującą na ekranie, jeśli pracujesz w miejscach publicznych?



Czy masz oddzielony profil prywatny od służbowego na telefonie?



Czy instalujesz tylko aplikacje niezbędne do pracy?



Czy pobierasz aplikacje wyłącznie z oficjalnych sklepów (Google Play, App Store)?



Czy regularnie sprawdzasz, jakie uprawnienia mają aplikacje (mikrofon, lokalizacja, kontakty)?



Czy usuwasz aplikacje żądające nieuzasadnionych dostępów?



Czy system i aplikacje są aktualizowane na bieżąco?