

Fundamenty bezpieczeństwa w każdej firmie

W niewielkiej firmie zajmującej się hostingiem zdjęć doszło do incydentu: pracownik odpowiedzialny za obsługę infrastruktury sieciowej, pracujący w tzw. open space, na swoim laptopie służbowym przeglądał zawartość stron z CSAEM. Zwrócił na to uwagę pracownik siedzący obok. Okazało się, że użytkownik laptopa, mając dostęp do niemonitorowanej sieci służbowej, wyszukiwał pliki zawierające CSAEM i NSFW, pobierał je i zapisywał na sprzęcie służbowym, katalogując w folderach o wymownych nazwach „7yo”, „nastolatki”, „teens”. Gdyby nie przypadek, być może nikt nie dowiedziałby się, jakiego rodzaju treści posiada pracownik IT. W firmie nie było procedury regularnego skanowania sprzętu i sieci pod kątem treści określanych mianem CSAEM (ang. Child Sexual Abuse and Exploitation Materials, pol. treści przedstawiające seksualne wykorzystywanie dziecka) oraz NSFW (ang. Not Safe For Work, pol. nieodpowiednie do przeglądania w miejscu pracy, tj. przemoc, pornografia, treści toksyczne). Nie było też osoby, która cyklicznie, manualnie przeprowadzałaby analizę zawartości dysków służbowych pod kątem nielegalnych plików. Sytuacja zakończyła się zabezpieczeniem laptopa i wszystkich sprzętów służbowych, do których ww. pracownik miał dostęp, audytem w całej firmie, który przeprowadził niezależny podmiot specjalistyczny, a równolegle zawiadomieniem organów ścigania i wszczęciem postępowania karnego przeciwko pracownikowi IT.

Bezpieczeństwo firmy to nie tylko *firewall*, kopie zapasowe czy silne hasła. Jednym z realnych – choć często pomijanych – zagrożeń jest obecność nielegalnych lub niepożądanych plików na sprzęcie służbowym oraz w sieci firmowej. Przykładowy incydent opisany powyżej pokazuje, że nawet w firmach IT, które mają wysoki poziom wiedzy technicznej, może dojść do sytuacji stwarzających poważne ryzyko prawne, reputacyjne i organizacyjne.

Ważne jest, żeby przedsiębiorstwo miało **systemowe, powtarzalne i udokumentowane** zasady dotyczące monitorowania sprzętu, kontroli treści oraz reagowania na incydenty. Brak takich procedur może prowadzić do:

- przechowywania materiałów nielegalnych na firmowych komputerach
- narażenia całej organizacji na odpowiedzialność karną i cywilną
- cofnięcia poświadczeń bezpieczeństwa i certyfikatów branżowych
- utraty zaufania klientów
- ryzyka sabotażu, wycieku danych lub szantażu

Tak jak w przypadku zarządzania sprzętem, podstawą jest **kontrola, transparentność i jasno określone zasady użytkowania urządzeń i sieci firmowych.**

Zarządzanie plikami i danymi na sprzęcie i w sieci firmowej

1. Jasna polityka korzystania ze sprzętu i sieci

Fundamentem jest spisana, obowiązująca i komunikowana pracownikom polityka korzystania z zasobów IT. Powinna ona zawierać m.in.:

- dopuszczalne i niedopuszczalne sposoby korzystania z Internetu
- zakaz pobierania i przechowywania nielegalnych plików (np. pliki zawierające treści przedstawiające seksualne wykorzystywanie dziecka, zoofilię, treści rasistowskie, itp.)
- informację o tym, że sprzęt służbowy nie służy do celów prywatnych
- zasady kontroli i monitorowania zasobów przez administratora
- opis konsekwencji: postępowanie dyscyplinarne, utrata poświadczeń bezpieczeństwa i certyfikatów, zawiadomienie krajowych lub zagranicznych organów ścigania (internetowe przestępstwa seksualne na szkodę małoletnich mają zazwyczaj charakter transgraniczny i ścigane są w większości jurysdykcji na świecie)

Należy pamiętać, że brak polityki to brak ram prawnych, do których można się odwołać.

2. Monitorowanie i filtrowanie ruchu sieciowego

Firma powinna wdrożyć środki kontroli sieci, aby zapobiegać sytuacjom, w których pracownik uzyskuje dostęp do nielegalnych treści. Mogą to być m.in.:

- filtrowanie stron internetowych (systemy blokujące domeny zawierające treści nielegalne, np. CSAEM, niepożądane lub ryzykowne, np. NSFW)
- rejestrowanie i zgłaszanie prób wejścia na zakazane witryny
- ograniczenie dostępu do niemonitorowanych lub nieautoryzowanych sieci Wi-Fi
- stosowanie segmentacji sieci (użytkownik ma dostęp tylko do tego, co jest niezbędne do realizacji zadań służbowych)
- wprowadzenie systemów DLP (ang. *Data Loss Prevention*) monitorujących, wykrywających i blokujących utratę danych (np. wysyłanie/odbieranie poufnych danych e-mailem, przechowywanie treści nielegalnych w chmurze firmowej)

Monitorowanie zawsze powinno odbywać się zgodnie z prawem i być opisane w politykach wewnętrznych.

3. Regularne skanowanie i audyt sprzętu służbowego

Komputery służbowe mogą być miejscem gromadzenia i przeglądania materiałów niezgodnych z prawem. Kontrola zawartości urządzeń nie może być doraźna (od incydentu do incydentu).

Dlatego organizacja powinna ustanowić procedury:

- **ewidencji sprzętu służbowego** (w tym dysków i pamięci przenośnych)
- **cyklicznego skanowania dysków i pamięci przenośnych** (z użyciem narzędzi wykrywających, np. treści przedstawiające seksualne wykorzystywanie dzieci oraz wzorce ryzykownych zachowań, np. księgowy czy manager produkcji odwiedzający stron www i pobierający nielegalne pliki audiowizualne)
- **analizy zawartości folderów użytkowników i ich nazw**, w tym katalogów tymczasowych i domyślnej lokalizacji do pobierania danych (lokalizacje specyficzne dla poszczególnych systemów operacyjnych)
- **okresowego raportowania podejmowanych działań i ich wyników** (nawet tych o neutralnym znaczeniu dla bezpieczeństwa firmy), a **dodatkowo**, kiedy wykryto incydent
- **skanowania sprzętu** przed przekazaniem kolejnemu pracownikowi lub przed jego utylizacją

Kontrola powinna być systemowa, a nie incydentalna.

4. Zarządzanie uprawnieniami i nadzorem nad administratorami

Pracownicy z uprawnieniami administracyjnymi mają większe możliwości techniczne, a tym samym mają większy dostęp do infrastruktury sieciowej firmy, mogą obchodzić filtry i ukrywać niepożądane działania lub treści. Dlatego:

- dostęp administracyjny powinien być przyznawany tylko wtedy, gdy jest konieczny
- wszystkie konta uprzywilejowane muszą być rozliczalne (logi, pełna identyfikacja użytkownika, brak możliwości usuwania historii aktywności)
- firma powinna stosować zasadę najmniejszego uprzywilejowania (ang. *least privilege*)
- działania administratorów (i oczywiście każdego użytkownika, w tym kierownictwa) powinny być monitorowane, logi zabezpieczone przed modyfikacją, a także archiwizowane zgodnie z przyjętą polityką bezpieczeństwa, np. na potrzeby audytu bezpieczeństwa lub postępowania karnego

5. Procedura reagowania na incydent

Gdy pojawia się podejrzenie, że na sprzęcie służbowym mogą znajdować się treści nielegalne, firma powinna działać według ustalonego schematu dostosowanego do rodzaju podmiotu. Poniżej przykładowa procedura:

1. **Powiadomienie o zaistniałym incydencie** – zgodnie z przyjętą polityką bezpieczeństwa firmy – niezbędnego minimum osób/działów (np. kierownictwo, dział prawny, dział bezpieczeństwa, IODO, HR).

2. **Zabezpieczenie sprzętu i danych** niezwłocznie po zaistnieniu i ujawnieniu incydentu (bez zmiany jego zawartości).
3. **Odłączenie urządzenia od sieci** w celu zatrzymania pobierania lub przesyłania danych. *
4. **Dokumentowanie czynności** (minimum: kiedy, w jaki sposób, kto zabezpieczył sprzęt i dane).
5. **Przekazanie urządzenia osobie/działowi odpowiedzialnej(-go) za bezpieczeństwo firmy**, a w razie podejrzenia przestępstwa – **niezwłoczne zawiadomienie organów ścigania**.
6. **Przeprowadzenie audytu** w pozostałych zasobach firmy.
7. **Wdrożenie działań naprawczych**, żeby zapobiec powtórzeniu incydentu.

* kolejność realizacji pkt 1-3 powinna być adekwatna do rodzaju zaistniałego incydentu

Najważniejsze zasady:

- jasna i aktualna polityka korzystania ze sprzętu i sieci
- monitorowanie i filtrowanie ruchu sieciowego
- regularne skanowanie i audyt urządzeń służbowych
- rozliczalność kont uprzywilejowanych
- zabezpieczanie sprzętu zgodnie z procedurą w razie incydentu
- szkolenia pracowników w zakresie odpowiedzialnego korzystania ze sprzętu IT

Checklista: zapobieganie nielegalnym i niepożądanym treściom w firmie – pytania kontrolne

- Czy obowiązuje przejrzysta i kompleksowa polityka korzystania z urządzeń i sieci firmowych?
- Czy w firmie funkcjonują ustandaryzowane zasady zarządzania kontami administratorów i użytkowników?
- Czy dostęp do zasobów firmowych jest kontrolowany, a zdarzenia są rejestrowane w logach?
- Czy istnieje i jest znana procedura reagowania na incydenty bezpieczeństwa związane z treściami nielegalnymi lub niepożądanymi?
- Czy pracownicy są regularnie szkoleni w zakresie bezpiecznego i zgodnego z zasadami korzystania ze sprzętu oraz sieci firmowej?

- Czy prowadzony jest monitoring ruchu sieciowego pod kątem podejrzanej aktywności?
- Czy w sieci formowej wdrożone jest filtrowanie stron i kategorii treści?
- Czy istnieje procedura cyklicznego skanowania i audytu urządzeń pod kątem nielegalnych treści CSAEM lub innych niepożądanych plików?