Czy warto monitorować pracowników?

Większość pracodawców postrzega monitorowanie osób zatrudnionych jako sposób na podniesienie wydajności ich pracy. Z kolei pracownicy nierzadko obawiają się tego typu kontroli i traktują ją jako jedną z metod inwigilacji. Czy na pewno chodzi tu o podglądanie?

Wnikliwe kontrolowanie poczynań podwładnych i poprawa efektywności wykorzystania powierzonego im sprzętu komputerowego oraz oprogramowania przekładają się na lepsze wyniki organizacji, realizację założonych celów i tym samym sukces firmy. Czy przy okazji nie ucierpią relacje w zespole, wzajemne zaufanie, dobra atmosfera czy kreatywność?

SKUTECZNE NARZĘDZIE

Oprogramowanie do monitorowania pracowników może pomóc zwiększyć wydajność pracy, nigdy jednak nie zastąpi skutecznego zarządzania przez cele. Nie da się procesów i działań realizowanych przez menedżerów sprowadzić do suchego wyliczenia i porównywania liczby godzin aktywnie przepracowanych przy komputerze. Eksperymenty przeprowadzone w wielu firmach pokazują, że samo poinformowanie pracowników o tym, że ich praca przy komputerze będzie monitorowana, działa bardzo mobilizująco – spada liczba wydruków, mniej osób w czasie pracy korzysta z portali społecznościowych i załatwia prywatne sprawy. Inny punkt widzenia reprezentują osoby odpowiedzialne za infrastrukturę teleinformatyczną w firmie. Dla nich wydajność pracowników nie ma większego znaczenia – najważniejszym aspektem monitoringu jest bezpieczeństwo IT oraz możliwość ograniczania szkodliwych, często nieumyślnych, działań pracowników. Jedynie w uzasadnionych przypadkach, gdy np. zachodzi podejrzenie wystąpienia incydentu zagrażającego bezpieczeństwu czy dobremu imieniu firmy, zebrane dane mogą być szczegółowo analizowane oraz można skorzystać np. z opcji cyklicznego wykonywania zrzutów ekranowych. W skrajnych sytuacjach pozwala to na skuteczne gromadzenie dowodów elektronicznych.

OCHRONA DANYCH, MINIMALIZACJA STRAT

Jednym z najważniejszych aspektów związanych z bezpieczeństwem jest ochrona danych. Obecnie firmy gromadzą coraz większe ilości informacji przy jednoczesnej dywersyfikacji urządzeń, na których są one przetwarzane. Zagwarantowanie bezpieczeństwa poufnych danych w tak zmiennym i wymagającym otoczeniu często jest wyzwaniem. – Niestety wiele firm uważa, że samo inwestowanie w zaawansowane rozwiązania technologiczne gwarantuje wystarczającą ochronę danych. Jednak nie wolno zapominać, że zagrożenia związane z utratą lub kradzieżą danych pochodzą z bardzo różnych źródeł – mogą to być zarówno cyberataki, świadome działania użytkowników, jak i zupełnie przypadkowo popełnione błędy. W sytuacji gdy napastnik uzyska nieautoryzowany dostęp do systemu, może zakłócić działanie usług, zablokować funkcje systemu lub zmienić, usunąć albo wykraść cenne informacje – tłumaczy Grzegorz Oleksy, dyrektor firmy Axence oferującej oprogramowanie nVision do monitorowania bezpieczeństwa sieci firmowej. Wbrew powszechnemu mniemaniu często o wiele większe straty powodują wewnętrzne zaniedbania w firmie i tzw. czynnik ludzki niż ataki hakerów. Ubiegłoroczny raport Fortinet pokazał też, że aż 42% więcej osób (w porównaniu z danymi z 2012 r.) jest gotowych złamać korporacyjne zasady korzystania z własnych urządzeń w miejscu pracy. W obliczu tych danych, zwiększonej mobilności pracowników oraz popularyzacji trendu BYOD (pracy na prywatnych urządzeniach) przedsiębiorstwa powinny przywiązywać większą wagę do stosowania zabezpieczeń w zakresie całej infrastruktury. Utrata ciągłości operacyjnej może wiązać się z utratą klientów i pozycji na rynku, a wyciek poufnych danych osobowych, zgodnie z art. 51 ustawy o ochronie danych osobowych, podlega grzywnie, karze ograniczenia wolności lub pozbawienia wolności do lat dwóch. Zabezpieczenie się przed krytycznymi sytuacjami przekłada się na wiele oczywistych korzyści dla firmy – pozwala na sprawne funkcjonowanie organizacji, brak problemów natury prawnej czy konieczności ponoszenia niepotrzebnych wydatków. Stosowanie wysokiej jakości oprogramowania kompleksowo monitorującego infrastrukturę IT i zabezpieczającego dane przed wyciekiem nie tylko podnosi poziom bezpieczeństwa wewnątrz organizacji, ale może zadecydować o tym, że klient postawi właśnie na tę, a nie inną firmę jako zaufanego kontrahenta.

Grzegorz Oleksy
dyrektor firmy Axence, producenta oprogramowania nVision do monitorowania bezpieczeństwa sieci firmowej

Wdrażając monitorowanie pracowników w organizacji, należy pamiętać, że sama kontrola nie wystarczy. Nie chodzi nam przecież o to, żeby jedynie sprawdzać wstecz, co się wydarzyło, analizować i wyciągać konsekwencje. Każdemu pracodawcy powinno przede wszystkim zależeć na zapobieganiu zagrożeniom – skuteczniej jest przeciwdziałać, a nie leczyć. Zadbajmy więc o odpowiednie przeszkolenie pracowników w zakresie zasad i reguł polityki bezpieczeństwa firmy, ochrony danych, regulaminu IT itp. Zapewnijmy im stały dostęp do dokumentów zawierających powyższe wytyczne. Odpowiadajmy na pytania, rozwiewajmy wątpliwości i udzielajmy rad, jak na co dzień spełniać założenia regulaminów bezpieczeństwa. Bez takiego przygotowania samo monitorowanie po prostu nie będzie miało sensu.