Przełamać stereotyp, czyli o dobrych praktykach w monitorowaniu pracowników... i wspólnych korzyściach.

Jakub Kralka,
Inżynier Sprzedaży Axence

Monitorowanie aktywności na komputerach pracowników nadal wzbudza kontrowersje, choć wdrożone mądrze i z poszanowaniem praw jednostki, pomaga firmom i instytucjom zwiększyć bezpieczeństwo oraz wydajność pracy. Gdy wynik finansowy organizacji wzrasta, korzyści czerpią wszyscy pracownicy, choć część z nich zazwyczaj głośno protestuje przed wprowadzeniem narzędzi monitorujących. Czy mają się czego obawiać? Jak z nimi rozmawiać, by zrozumieli, że mogą tylko zyskać?

Monitorowanie aktywności użytkowników sieci to w Polsce nadal wrażliwy temat. Historia najnowsza kraju, w którym zaledwie trzy dekady temu funkcjonowały mechanizmy rodem z powieści Orwella, wpływa na negatywne postrzeganie oprogramowania do monitorowania aktywności użytkowników. Nie tylko skojarzenia z praktykami poprzedniego systemu budzą niechęć do tego typu rozwiązań. Jest za to odpowiedzialna także niedostateczna edukacja. Mało osób ma świadomość po co dokładnie wprowadza się narzędzia monitorujące ich pracę. Przecież mamy sobie ufać. Czy powinniśmy się obawiać wprowadzenia rozwiązań, które w rozwiniętych gospodarkach stanowią integralną część funkcjonowania przedsiębiorstw, a co najważniejsze, akceptowaną i traktowaną przez pracowników formą raportowania wyników pracy? Odpowiedź brzmi nie, ale zacznijmy od początku, czyli od idei, jaka przyświeca wprowadzeniu narzędzi do monitorowania aktywności użytkowników.

By najsłabsze ogniwo...

Podczas szkoleń, prezentacji i rozmów często prosimy o wskazanie „najsłabszego ogniwa" w łańcuchu ochrony firmowej sieci, a więc czynnika stwarzającego największe ryzyko zagrożeń i strat finansowych. Odpowiedź jest zawsze ta sama i brzmi: **użytkownik.** Niezależnie od tego, czy świadomie czy nieświadomie łamie on politykę bezpieczeństwa, tudzież wydajność jego pracy jest niska, konsekwencje zawsze obciążają rachunek pracodawcy.

Niestety niefrasobliwość pracowników skutkuje coraz większą liczbą ataków i wycieków danych. **Co 12 sekund 12 nowych urządzeń[1] zostaje zainfekowanych szkodliwym oprogramowaniem,** w tym ostatnio najbardziej popularnym typu Ransomware. Od 2005 do 2015 roku w USA zgłoszono 7700 przypadków tych ataków, a straty oszacowano na ok. 57,6 mln USD[2]. Łatwy zarobek spowodował wzrost popularności Ransomware i tylko w drugim kwartale 2015[3] roku zarejestrowano aż 4 miliony incydentów. Hakerzy nie atakują już bezpośrednio serwerów naszych organizacji, bo najbardziej skuteczne są najprostsze sposoby zainfekowania sieci. Odpowiedzmy sobie na pytanie co zrobimy, gdy pod drzwiami znajdziemy pozostawiony pendrive? No właśnie… W ten sposób wpuściliśmy do firmy złośliwe oprogramowanie. To tylko jeden z wielu scenariuszy, ponieważ malware jest preinstalowany na różnych, ładowanych przez port USB urządzeniach, które z łatwością można kupić w sieci. Cyberprzestępcy z Chin wgrywają złośliwy kod nawet na (sic!) e-papierosy[4].

Niestety korzystanie z nieautoryzowanych nośników danych to nie jedyne zagrożenie. Tylko w lutym 2016[5] roku odnaleziono 293 747 witryn wyłudzających dane użytkowników. Dane te mogą zawierać strategiczne informacje lub technologie tworzące przewagę danego podmiotu na rynku. Na takie witryny możemy być przekierowani, używając najbardziej popularnych serwisów społecznościowych. Jak wynika z raportów TimeCamp, pracownicy spędzają 1 godzinę i 11 minut dziennie m.in. na portalach niezwiązanych ze swoimi obowiązkami. Są wtedy szczególnie narażeni na atak z zewnątrz. Media społecznościowe są na obecną chwilę podstawowym kanałem promocji i dystrybucji oprogramowania do phishingu[6]. Celem takich ataków jest dotarcie do wąskiej grupy odbiorców i uzyskanie dostępu do ich serwisów lub danych.

Najważniejsze cele dla większości ataków phishingowych:

- instytucje finansowe,
- serwisy chmurowe / serwisy hostingowe,
- serwisy webmailowe oraz serwisy z usługami online,
- serwisy e-commerce,
- serwisy świadczące usługi płatnicze[7].

Przez nieautoryzowane działania użytkowników każda organizacja może stracić bardzo wiele, począwszy od pieniędzy, przez kluczowe zasoby, na wizerunku kończąc. Choć działy IT firm coraz częściej wyposażają się w systemy DLP (ang. Data Leak Prevention), oprogramowanie antywirusowe, firewalle czy sandboxy[8], bez świadomości dotyczącej zagrożeń nie może być mowy o stuprocentowej ochronie przed niebezpieczeństwem. Co wobec tego robić? Odpowiedź wydaje się prosta: edukacja, cykliczne szkolenia, pokazywanie pracownikom na co powinni uważać w sieci. To fakt, ale zagrożenia przybierają coraz trudniejszą do wykrycia postać i ewoluują tak szybko, że nasi pracownicy praktycznie nie wychodziliby ze szkoleń.

[1] http://visual.ly/truth-about-how-spyware-affects-you

[2] http://www.businessinsider.com/doj-and-dhs-ransomware-attacks-government-2016-4?IR=T

[3] http://www.securitymagazine.com/articles/86787-ransomware-attacks-to-grow-in-2016

[4] https://www.theguardian.com/technology/2014/nov/21/e-cigarettes-malware-computers

[5] https://www.wordfence.com/blog/2016/02/trends-malware-phishing/

[6] https://info.phishlabs.com/pti-report-download

[7] https://www.topsec.com/it-security-news-and-info/surprising-statistics-about-computer-viruses

[8] http://www.howtogeek.com/169139/sandboxes-explained-how-theyre-already-protecting-you-and-how-to-sandbox-any-program/

Jeśli da się zhackować konto szefa kampanii prezydenckiej Hillary Clinton[9], to można złamać każdego. Gdy atakujący jest zawsze o krok przed ofiarą, dodatkowo powinno się prewencyjnie monitorować zachowania narażonych na atak użytkowników sieci, by jak tylko się da zminimalizować ryzyko niebezpieczeństwa. Kluczem do sukcesu jest synergia tych trzech elementów: sprzętu IT security, wysokiej świadomości oraz dodatkowego obserwowania co dzieje się w naszej sieci z perspektywy jej użytkownika.

… stało się brakującym

W krajach dawnego bloku wschodniego monitorowanie jakiejkolwiek aktywności użytkowników jest nadal odbierane jako atak na prywatność, godność i poszanowanie praw jednostki, wynikające z litery prawa i gwarantowane przez chociażby Konstytucję RP[10]. Dlatego też wprowadzenie mechanizmów monitorowania aktywności użytkownika oraz tworzenie dzięki temu nowego systemu prewencji przed zagrożeniami z zewnątrz sieci, powinno być jasno i klarownie wyjaśnione każdemu pracownikowi z naciskiem na cel, który dzięki temu chce osiągnąć firma. Jeżeli spojrzymy na taką zmianę z punktu widzenia makro-otoczenia przedsiębiorstwa, dostrzeżemy jedynie pozytywne jej aspekty:

- możemy uzyskać/zaoszczędzić środki finansowe,
- podnieść bezpieczeństwo,
- zoptymalizować wiele procesów wewnątrz organizacji,
- dogonić/uciec konkurencji lub po prostu odnieść większy niż planowany sukces[11].

Większość ludzi nie lubi jednak zmian. Każde działanie zmierzające do naruszenia naszej personalnej strefy komfortu lub przyzwyczajeń uruchamia psychologiczne mechanizmy obronne, stawiające osoby, których zmiany dotyczą, w jawnej opozycji. Jest to pierwszy i całkiem naturalny odruch zakorzeniony głęboko w naszym mózgu, w jego najstarszych częściach rozwijanych jeszcze od czasów Homo Erectus, a pisał już o tym Freud. Niestety częstą konsekwencją poddania się temu odruchowi jest przejście do marazmu lub stagnacji, co prowadzi do całkiem odwrotnego niż zamierzony efektu wprowadzenia zmiany. „Opór materii" w kwestiach wdrożenia narzędzi do monitorowania aktywności użytkownika może zmniejszyć właściwa komunikacja.

[9] https://niebezpiecznik.pl/post/jak-zhackowano-szefa-kampanii-prezydenckiej-hillary-clinton/

[10] Konstytucja Rzeczpospolitej Polskiej z dnia 2 kwietnia 1997 r.: art. 47, art. 49, art. 51. Ustawa z dnia 26 czerwca 1974 r. Kodeks Pracy: art. 111, art. 15, art. 221, art. 94.

[11] http://www.wnp.pl/artykuly/dlaczego-boimy-sie-zmian-i-do-czego-to-prowadzi,7697.html

Niepowodzenia związane z wdrażaniem zmiany najczęściej ujawniają się w następujących obszarach:

1. Zarządzanie projektem **20,00%**,
2. Zarządzanie budżetem **29,00%**,
3. Brak kamieni milowych **34,00%**,
4. Brak kontroli **35,00%**,
5. Brak planowania **39,00%**,
6. Zła komunikacja **57,00%**[12].

Rekomendowana i sprawdzona już procedura wprowadzenia narzędzi monitorowania aktywności użytkownika sprowadza się do kilku kroków. Pierwszym etapem powinno być doprecyzowanie i klarowne przedstawienie powodów wprowadzenia monitorowania aktywności (obniżona wydajność pracowników, wysokie koszty wydruków zaobserwowane w ostatnim roku, nagminne łamanie polityki bezpieczeństwa, strata udziału w rynku w stosunku do konkurencji) oraz jaki jest jego cel. W większości przypadków można podzielić to na dwie grupy:

Monitorowanie Operacyjne (skierowane i przydatne dla działów IT)	Monitorowanie Planistyczne (skierowane i przydatne dla dyrekcji/zarządu)
• Zarządzanie awariami i przeciwdziałanie im • Zarządzanie konfiguracją sieciową • Zarządzanie bezpieczeństwem • Zarządzanie ryzykiem	• Zarządzanie wydajnością • Zarządzanie rozliczeniami • Zarządzanie zmianami • Zarządzanie ryzykiem

Dalsze kroki to kolejno: przypomnienie zasad korzystania z infrastruktury IT, przedstawienie planu wdrożenia narzędzia i przeszkolenie kadry z zasad jego funkcjonowania oraz zagwarantowanie minimalizacji możliwości naruszenia prywatności pracownika przez pracodawcę. Pamiętajmy, że istnieją odpowiednie zapisy mówiące o konieczności przekazania pracownikowi informacji o tym, iż jego aktywność może być monitorowana w czasie wykonywania obowiązków wynikających z umowy między podmiotami.

[12] http://www.wnp.pl/artykuly/dlaczego-boimy-sie-zmian-i-do-czego-to-prowadzi,-7697_0_0_0_0.html

„Rozporządzenie Ministra pracy i Polityki Społecznej Załącznik – pkt 10 lit. E
10. Przy projektowaniu, doborze i modernizacji oprogramowania, a także przy planowaniu wykonywania zadań z użyciem ekranu monitora pracodawca powinien uwzględnić w szczególności następujące wymagania:(…) e) bez wiedzy pracownika nie można dokonywać kontroli jakościowej i ilościowej jego pracy"[13]

Zakres i korzyści

Jakie uprawnienia posiada pracodawca w kwestiach monitorowania aktywności swoich pracowników? Są to m.in.:

- monitorowanie aktywności w internecie wraz z możliwością kategoryzowania treści,
- monitorowanie użycia łącza internetowego,
- monitorowanie czasu pracy użytkownika,
- monitorowanie wydruków,
- dostęp do zasobów na stacjach roboczych,
- monitorowanie wykorzystania aplikacji
- monitorowanie instalacji lub deinstalacji aplikacji,
- podgląd pulpitu,
- monitorowanie aktywności stacji roboczej.

Pozostałe metody, takie jak np. instalowanie keyloggera, czyli programu przechwytującego wszystko, co wpisuje się na klawiaturze, są zabronione.

Jakie korzyści może przynieść pracodawcy wdrożenie narzędzi monitoringu aktywności jego pracowników? To przede wszystkim mechanizmy edukacyjne budujące świadomość u użytkownika o potencjalnych zagrożeniach i jednoczesne przeciwdziałanie im. Wprowadzenie filtracji treści, jakie użytkownik przegląda w internecie, logując się na niebezpieczne witryny, można wzbogacić odpowiednimi komunikatami wyjaśniającymi powód blokowania konkretnej domeny czy adresu IP (strona wyłudzająca dane lub zawierająca treści nieodpowiednie np. pliki zabezpieczone prawem autorskim lub pornograficzne). Działania te wspierają procesy zarządzania ryzykiem i są częścią wprowadzenia inteligentnej i skutecznej polityki bezpieczeństwa.

[13] Rozporządzenie Ministra Pracy i Polityki Socjalnej z dnia 1 grudnia 1998 r. w sprawie bezpieczeństwa i higieny pracy na stanowiskach wyposażonych w monitory ekranowe.

Kolejna policzalna zaleta to wzrost wydajności pracownika. Badania pokazują, że od momentu poinformowania kadry o stosowaniu oprogramowania monitorującego aktywność – pracownicy poświęcają średnio **90 minut dziennie** więcej na wykonywanie obowiązków służbowych[14].

Spróbujmy poddać to pewnej symulacji: Firma X zatrudnia 100 pracowników, z czego 60 z nich to pracownicy biurowi, wykonujący swoją pracę przy stanowiskach komputerowych. Przyjmijmy, iż posiadają oni minimalną gwarantowaną od 2017 roku godzinową stawkę płacy. Ile zaoszczędzi pracodawca na eliminacji tzw. cyberslackingu[15] ?

60 pracowników **x 1,5** h dziennie **x 12** zł **x 20** dni w miesiącu **x 12** miesięcy

= ~ 259 200 zł w skali roku!!

Niezależnie od kultury organizacyjnej częstym zjawiskiem jest drukowanie prywatnych materiałów na firmowym sprzęcie. Jeden z klientów, który wdrożył rozwiązanie klasy Axence nVision pochwalił się roczną oszczędnością rzędu 6000 zł netto na samych wydrukach.

Nawiązując stosunek pracy wzorowy Jan Kowalski powinien mieć świadomość, że jako firma wszyscy grają do jednej bramki. Cele mogą być różne i niezależnie czy jest to wzrost przychodów, umocnienie pozycji rynkowej czy ekspansja za granicę, każdy pracownik powinien uczestniczyć w ich realizacji. Jeśli bowiem cele zostają spełnione, możliwy będzie jego rozwój: awans, podwyżka, poprawienie warunków pracy. To podstawowa motywacja. Nie możemy jednak założyć, że każdy wzorowy Jan Kowalski przez przypadek nie wpuści do firmy wirusa, który spowoduje jej bankructwo, a taki scenariusz również jest możliwy i głośno było o przypadkach upadku przedsiębiorstwa przez awarię IT. Nie możemy również zakładać, że zrekrutujemy samych wzorowych Janów Kowalskich. Po podpisaniu umowy mogą bowiem zdjąć maskę i pracować na naszą niekorzyść. Monitorowanie ich pracy w służbie bezpieczeństwa sieci i niezakłóconego rozwoju jest w dzisiejszych czasach koniecznością, a jak wspomniano wcześniej, na świecie już dawno zauważoną praktyką, z którą w ramach umowy społecznej godzą się pracownicy. Takie kraje jak Japonia czy USA są nadal niedoścignionym wzorcem budowania kultury organizacji. Philip B. Crosby i jego TQM, William Deming i jego statystyczne sterowanie procesami, Bob Galvin i jego Six Sigma, stworzyły fundamenty pod funkcjonowanie największych gospodarek globu. Kraje te już dawno temu mierzą wydajność procesów produkcji czy pracowników i opierają swoje mechanizmy zarządzania i planowania strategicznego o kluczowe wskaźniki efektywności, dostarczane przez m.in. przez narzędzia do monitorowania aktywności użytkowników sieci.

[14] http://www.bostonglobe.com/business/2016/02/18/firms-step-monitoring-employee-activities-work/2l5hoCjsEZWA0bp10BzPrN/story.html

[15] http://kadry.infor.pl/kadry/hrm/zarzadzanie/669629,Co-to-jest-cyberslacking.html