Ile kosztuje złe zarządzanie IT?

Optymalizacja procesu zarządzania infrastrukturą IT niesie ze sobą szereg korzyści biznesowych. Najważniejszą z nich jest obniżenie zarówno aktualnych, jak i potencjalnych kosztów prowadzenia działalności. Ile można zyskać, wdrażając odpowiednie narzędzia i polityki w tym zakresie? Jak wiele można stracić na niewłaściwym zarządzaniu IT?

Awaria sieci warta miliony

Badania przeprowadzone przez IDC[1] wykazały, że przeciętny czas przerw spowodowanych awariami sieci, systemów komputerowych oraz aplikacji w firmach i instytucjach średniej wielkości to 11 godzin rocznie. Koszty przestojów w badanych podmiotach sięgały 10 000 USD za każdą godzinę. Największe przedsiębiorstwa, zdaniem analityków Gartnera[2] , w czasie awarii infrastruktury IT **mogą tracić nawet do 300 000 USD na godzinę**. Długotrwała niedostępność systemów IT może spowodować wielomilionowe straty, o czym przekonały się między innymi linie lotnicze Delta[3] oraz Southwest Airlines Co. Dla wielu mniejszych firm, niedysponujących dużymi rezerwami budżetowymi, taki przestój może oznaczać nawet bankructwo. British Chambers of Commerce w swoich raportach podaje, że 93% firm, które straciły dane w wyniku awarii IT na więcej niż 10 dni, ***zniknęło z rynku w ciągu roku*** od wystąpienia zdarzenia.

Jak minimalizować ryzyko?

Nawet największe i najlepiej zabezpieczone organizacje muszą liczyć się z faktem, że nie istnieje stuprocentowe zabezpieczenie przed potencjalnymi awariami, gdyż mogą być one również wynikiem działania sił wyższych w postaci np. trzęsienia ziemi czy huraganu. Można jednak w dużym stopniu wyeliminować przewidywalne zagrożenia, takie jak awarie wadliwego sprzętu, a nawet pożary w serwerowni. IDC w cytowanym wcześniej badaniu podaje, że konsekwentne **korzystanie z oprogramowania do zarządzania IT minimalizuje kosztowne awarie sieci i systemów komputerowych aż o 65%**. Dzięki narzędziom monitorującym stan infrastruktury, administrator sieci może uzyskać wiedzę np. o stanie serwisów, kondycji dysków twardych, a przy wykorzystaniu dodatkowych czujników także o temperaturze i wilgotności w serwerowni.

Najsłabsze ogniwo w systemie bezpieczeństwa

Przysłowiowa złośliwość rzeczy martwych to jedno ze źródeł awarii infrastruktury IT, a tym samym potencjalnych kosztów, których można uniknąć. Kolejnym jest nieautoryzowane działanie pracowników. W jednym z raportów Gartnera[4] czytamy, że **80% przerw w działaniu usług o znaczeniu krytycznym spowodowanych jest przez nieuprawnione zachowania użytkowników.** Pracownicy są często odpowiedzialni za wyciek strategicznych danych czy nieświadome wpuszczenie do sieci wirusów lub oprogramowania szpiegowskiego. Edukacja czasem nie wystarcza, dlatego polityka bezpieczeństwa firmy powinna zawierać zapisy o prewencyjnym monitorowaniu potencjalnie szkodliwych działań kadry. Należy także wyposażyć dział IT w odpowiednie narzędzia.

---

[1] https://www.mercurymagazines.com/pdf/IDC_RiskAssessment_WP_Final.pdf

[2] http://blogs.gartner.com/andrew-lerner/2014/07/16/the-cost-of-downtime/

[3] http://www.businessinsider.com/r-delta-says-flights-grounded-nationwide-after-system-outage-2016-8?IR=T

[4] https://img2.insight.com/graphics/no/info2/insight_art6.pdf

Oprogramowanie, które zaraportuje administratorowi podejrzane zachowania użytkowników, stanowi świetne uzupełnienie dla systemów bezpieczeństwa i programów antywirusowych. Należy przy tym pamiętać, że ***celem jego wykorzystania nie jest inwigilacja, tylko podniesienie poziomu ochrony*** *firmy przed wyciekami danych i atakami z zewnątrz. Rozwiązania programowe do zarządzania IT, wspierane przez moduł do monitorowania aktywności użytkowników, to słuszny wybór gdy chcemy ochronić swój biznes przed dużymi stratami pieniędzy, wynikającymi z nieautoryzowanych działań pracowników.*

–podkreśla Marcin Matuszewski,
Starszy Specjalista Pomocy Technicznej w Axence.

Wdrożenie narzędzi do monitorowania aktywności pracowników to nie tylko wzmocnienie łańcucha ochrony sieci, ale także zwiększenie wydajności zatrudnionych, a tym samym potencjalnie wyższy zysk, jaki można wygenerować w danym przedziale czasu. Dla przykładu firma z branży IT, zatrudniająca 5000 osób, po wdrożeniu monitorowania pracowników powiększyła roczny zysk o 2 miliony USD[5] . Ponadto od momentu poinformowania kadry o stosowaniu oprogramowania, poświęcają oni dziennie średnio 90 minut więcej na wykonywanie obowiązków służbowych. Sama świadomość bycia monitorowanym sprawia, że nie zajmują się prywatnymi sprawami w czasie pracy, niezależnie od tego, że administrator nie śledzi ich każdego kroku, a tylko otrzymuje informacje o podejrzanych aktywnościach.

Kosztowne licencje

Awarie sprzętu i aplikacji czy niebezpieczne zachowania użytkowników to nie jedyne zdarzenia, których efekty mogą poważnie zaszkodzić organizacji w wymiarze finansowym i wizerunkowym. Wysokie ryzyko stwarza także niewłaściwe zarządzanie licencjami na wykorzystywane oprogramowanie. W mediach głośno było o przypadku firmy ze wschodniej Polski, która musiała zapłacić **karę w wysokości miliona USD**[6] . W jej sieci znaleziono ponad 200 nielegalnych kopii programów. Wyposażony w odpowiednie oprogramowanie administrator jest w stanie szybko przeprowadzić audyt wykorzystywanych aplikacji i zobaczyć, które z nich nie posiadają ważnej licencji. Pozyskana wiedza pozwoli mu podjąć decyzję, które licencje dokupić, a które programy odinstalować.Równie ważna jest wiedza o stopniu wykorzystania poszczególnych licencji, którą także można zdobyć dzięki oprogramowaniu do inwentaryzacji zasobów IT. Na jej podstawie administrator łatwiej zdecyduje, które licencje są zbędne tzn. firma płaci za nie, a program nie jest używany. Dla przykładu Government Accountability Office ze Stanów Zjednoczonych, odpowiednik polskiej Najwyższej Izby Kontroli, stwierdził po audycie, że właściwe zarządzanie licencjami na oprogramowanie może przynieść olbrzymie oszczędności w sektorze publicznym. Jedna z głównych agencji federalnych w USA (nazwy nie ujawniono), zaraportowała, że tylko w 2012 roku udało jej się oszczędzić z tego tytułu 181 milionów USD[7] .

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

[6] https://bezprawnik.pl/rekordowy-milion-usd-odszkodowania-za-pirackie-oprogramowanie-w-polskiej-firmie/

[7] http://www.gao.gov/products/D07403

Zarządzanie z głową

Kompleksowe zarządzanie siecią pozwala zminimalizować ryzyko kosztownych przestojów i wycieków danych oraz uniknąć kar za posiadanie nielegalnego oprogramowania. Co więcej przyczynia się do skrócenia czasu i wzrostu wydajności pracy specjalistów, a tym samym redukuje koszty stałe. Dane zebrane przez instytucje badawcze oraz przypadki firm i instytucji z całego świata pokazują, że aby znacznie zwiększyć zyski w bilansie, warto rozważyć wdrożenie odpowiednich narzędzi do monitorowania sieci oraz jej użytkowników, a także inwentaryzacji sprzętu i oprogramowania. Na rynku istnieją rozwiązania all-in-one, które pozwalają skutecznie zaadresować wszystkie te obszary z poziomu jednej konsoli. Co więcej zawierają one mechanizmy, dzięki którym część procesów da się zautomatyzować tak, by skupiać uwagę zarządzającego jedynie na ważnych alertach.

Koszty
niewłaściwego zarządzania IT

Średnio **11 godzin** pracy rocznie traci każda firma przez przerwy spowodowane awariami infrastruktury IT.

źródło: IDC

Nawet **300 000 USD** może kosztować 1 godzina przestoju spowodowana awarią IT.

źródło: Gartner

93% firm, które straciły swoje dane w wyniku awarii IT, upadło w ciągu 1 roku.

źródło: British Chambers of Commerce

80% przerw w działaniu usług o znaczeniu krytycznym jest spowodowanych przez nieuprawnione zachowania użytkowników.

źródło: Gartner

1 mln USD musiała zapłacić firma ze wschodniej Polski za nielegalne oprogramowanie.

źródło: BSA The Software Alliance

Korzyści
z wdrożenia oprogramowania do zarządzania IT

Wdrożenie oprogramowania do zarządzania IT pozwala zminimalizować awarie infrastruktury o **65%**.

źródło: IDC

2 mln USD zarobiła w rok firma zatrudniająca 5000 osób dzięki oprogramowaniu do monitorowania aktywności pracowników.

źródło: Boston Globe

Po wdrożeniu oprogramowania do monitorowania aktywności pracowników, poświęcają oni dziennie średnio **90 minut** więcej na wykonywanie swoich obowiązków.

źródło: Boston Globe

Jedna z głównych agencji federalnych w USA zaraportowała, że tylko w 2012 roku oszczędziła na inwentaryzacji oprogramowania **181 milionów USD**.

źródło: Government Accountability Office

Administratorzy w rozmowach często podkreślają, że zarządzanie infrastrukturą za pomocą jednego kompleksowego narzędzia jest dla nich łatwiejsze i szybsze, ponieważ nie muszą wdrażać się w różne systemy, a później przełączać się między nimi. To ważne, zwłaszcza przy dużych sieciach złożonych z kilkuset stacji roboczych. To kolejny argument przemawiający za wdrożeniem narzędzia all-in-one, które pozwoli administratorowi oszczędzić czas i skupić się na innych, ważnych aspektach swojej pracy.

– dodaje Marcin Matuszewski z Axence.