BEZPIECZNY BIZNES

Firma bezpieczna w cyberprzestrzeni wymaga skutecznych narzędzi prawnych, a także wiedzy, jak i kiedy ich użyć

Przedsiębiorstwa coraz częściej stawiają w swoich strategiach na technologię, która pozwala im się szybciej rozwijać, ale zarazem naraża je na coraz większe zagrożenia. Oparte na najnowocześniejszych rozwiązaniach IT sprzedaż online, analiza danych, algorytmy, sztuczna inteligencja, Internet rzeczy, blockchain, automatyzacja i robotyzacja zyskują na znaczeniu, lecz jednocześnie zwiększają ryzyko związane z cyberzagrożeniami i dają ogromne pole do działań przestępczych.

Jacek **Bogiel**
prezes zarządu, Availo

Bezpieczeństwo w cyberprzestrzeni jest dziś niezbędne dla funkcjonowania całej gospodarki, ale dla sektora finansowego ma ono znaczenie fundamentalne: warunkuje egzystowanie i rozwijanie działalności przedsiębiorstwa. Podmioty z sektora consumer finance każdego dnia stoją przed wyzwaniem chronienia własnej infrastruktury umożliwiającej korzystanie z szeroko rozumianego Internetu i technologii cyfrowych, a ponadto gwarantować muszą ochronę integralności gromadzonych i przechowywanych danych, co wiąże się z zabezpieczeniem własności intelektualnej i tajemnicy przedsiębiorstwa.
Cyberbezpieczeństwo to jednak nie tylko zabezpieczanie techniczne systemów informacyjnych przed działaniami naruszającymi poufność, poprawność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług, to także przygotowanie narzędzi prawnych – z jednej strony umożliwiających zapobieganie atakom cybernetycznym, a z drugiej – wspierających proces niwelowania ich skutków.

Znaczenie wewnętrznych procedur

Istotnym obszarem ochrony przed cyberzagrożeniami jest przygotowanie i wdrożenie przez przedsiębiorstwo wewnętrznych procedur umożliwiających wykrywanie, rejestrowanie, analizowanie i klasyfikowanie sygnałów dotyczących bezpieczeństwa, a następnie podejmowanie działań naprawczych bądź działań zmierzających do ograniczenia skutków incydentów, które miały już miejsce.
Przedsiębiorstwa sektora consumer finance dołożyć muszą wszelkich starań, by dobro prawne w postaci danych było jak najlepiej chronione. W tym celu najczęściej wdrażają rozwiązania technologiczne: aplikacje i zabezpieczenia, przeprowadzają szkolenia pracowników dotyczące reagowania np. w przypadku wątpliwości co do prawdziwości przedkładanych dokumentów, szkolenia programistów w zakresie wymogów bezpieczeństwa dla architektury rozwiązań IT. Jednak ogromnie dużo zależy od samych użytkowników, czyli od klientów przedsiębiorstw. Istotna jest ich reakcja na przypadki przestępstw przeciw ochronie informacji, świadomość konieczności złożenia zawiadomienia o możliwości popełnienia przestępstwa, gotowość do współpracy z usługodawcą, do natychmiastowego zastrzeżenia dostępów i haseł. Warto zatem bardzo mocno postawić na edukację klientów. Komunikat powinien być prosty, zachęcający do lepszej ochrony urządzeń elektronicznych, do korzystania z zabezpieczonych stron, do czytania (jeszcze przed udzieleniem zgody na zainstalowanie oprogramowania) regulaminów i licencji, niezaznaczania bezwiednego akceptacji tych dokumentów, bo nieznajomość prawa szkodzi. Istotne jest ostrzeganie klientów przed udostępnianiem takich dokumentów jak dowód osobisty czy prawo jazdy. Jeśli nie jest to wymagane przepisami prawa, należy czuwać nad nimi z podobnym pietyzmem, jak czuwamy nad hasłami do bankowości internetowej. Obsługujący klientów pracownicy powinni ich wyczulać na konieczność używania silnych haseł, nieudostępniania ich nieznanym osobom, natychmiastowego zawiadamiania odpowiednich podmiotów w przypadku wystąpienia wszelkich zdarzeń budzących zastrzeżenia konsumenta usługi. Warto zadbać o to, by nie tylko świadczące usługę finansową przedsiębiorstwo i jego pracownicy, ale także klient miał świadomość, jak przeciwdziałać możliwym incydentom, a gdy już do nich dojdzie, co robić, by w jak największym stopniu zminimalizować skutki naruszenia.

Po wsparcie do specjalistów

O ile wiedzy na temat aspektów technologicznych bezpieczeństwa w sieci szukać należy u specjalistów od cyberbezpieczeństwa, o tyle po wiedzę o niezbędnych w walce z zagrożeniami tego typu narzędziach prawnych sięgać należy do wyspecjalizowanych firm prawniczych, adwokatów i radców prawnych.
W przestrzeni prawnej zdefiniowane zostały następujące przestępstwa przeciwko ochronie informacji:

- nieuprawnione uzyskanie informacji, czyli hacking (art. 267 §1 kk),
- podsłuch komputerowy, czyli sniffing (art. 267 §2 kk),
- niszczenie danych informatycznych (art. 268 a kk),
- uszkodzenie danych informatycznych (art. 269 kk),
- zakłócenie systemu komputerowego (art. 269 kk),
- uruchomienie impulsów telefonicznych (art. 285 kk),
- oszustwo popełniane za pośrednictwem Internetu (art. 286 kk),
- oszustwo komputerowe (art. 287 kk),
- paserstwo programu komputerowego (art. 293 kk),
- spaming (art. 24 u.ś.u.d.e),
- fałszerstwa dokumentów i podpisów oraz wyłudzenia kredytów.

Wyspecjalizowane firmy prawnicze z branży prawo direct zapewniają nieodzowne wsparcie w postaci porad prawnych bądź przygotowania dokumentów – w zakresie wszystkich powyższych obszarów, w sprawach znajdujących się na etapie przedprocesowym. Pakiety porad prawnych mogą być integralną częścią oferty kierowanej do klienta przez podmiot świadczący usługę finansową. Kompleksowe rozwiązania tego typu już funkcjonują na rynku i cieszą się rosnącą popularnością.
Na koniec warto podkreślić, że w zależności od dostawcy usług i rodzaju tych usług prawo nakłada na podmioty finansowe szereg obowiązków, w szczególności w zakresie informowania o usługach płatniczych czy prawach i obowiązkach stron wynikających z umów o świadczenie usług płatniczych. Pracownicy instytucji finansowych powinni bądź samodzielnie sprawnie poruszać się po tych przepisach, bądź też mieć możliwość zasięgnięcia porady w celu ochrony podmiotu oraz swoich klientów. Własne procedury, regulamin i zabezpieczenia pomogą z pewnością uchronić zarówno samo przedsiębiorstwo, jak i jego klientów przed atakami cyberprzestępców.

BEZPIECZNY BIZNES

Zabezpieczone płatności mobilne i elektroniczne. Kto gwarantuje bezpieczeństwo klientom?

Sposób, w jaki się komunikujemy, wdrażamy innowacje czy robimy zakupy, zmienia się obecnie szybciej niż dotychczas. Rozwój technologiczny, rosnąca liczba operacji i transakcji internetowych oraz zawrotne tempo życia stwarzają jednak nowe okoliczności dla cyberprzestępców.

Jakub **Czerwiński**
VP Sales CEE, Adyen

Wszystkie przedsiębiorstwa, które chcą utrzymać się na szczycie biznesowej gry, stają się coraz bardziej mobilne i technologiczne (także w kontekście płatności). Wraz z procesem transformacji biznesu opartej na technologiach, zwiększa się także skala i wachlarz zagrożeń, ponieważ cyberprzestępcy podejmują kolejne kroki, by na bieżąco śledzić firmy i ich klientów. Niepokojące jest to, że niektóre z nich nadal nie zrobiły nic, aby chronić swoje strony internetowe, aplikacje, wirtualne sklepy i dane konsumentów.

Lepiej zapobiegac niż leczyć

Zagrażające bezpieczeństwu działania w sieci są zazwyczaj dokonywane dla osobistego zysku atakujących. Obejmują m.in. nieautoryzowane transakcje, pozyskiwanie wrażliwych danych, fałszywe wnioski o zwrot pieniędzy, tworzenie alternatywnych treści zachęcających do określonych czynności itp. Z tego powodu obowiązkiem sprzedawców powinno być ograniczenie liczby nieuczciwych działań i ochrona swoich klientów. Upewnienie konsumentów, że ich dane są bezpiecznie przetwarzane, to jeden z najważniejszych czynników budowania pozycji wobec konkurencji.

Zapewnienie bezpieczeństwa wszystkich procesów wymaga dużego wysiłku i energii, ale niezatrzymane oszustwa zawsze generują znacznie więcej kosztów i mają bardzo szkodliwy wpływ na wiarygodność firmy oraz zaufanie klientów. Nowe rodzaje przestępstw przyprawiają przedsiębiorców o jeszcze większy ból głowy, ponieważ strategie mające na celu kradzież pieniędzy lub informacji stają się bardziej skomplikowane z każdym dniem, a używane w tym celu narzędzia i sztuczki socjotechniczne coraz bardziej zaawansowane. By odpowiednio zarządzać procedurami związanymi z cyberbezpieczeństwem firmy, warto rozważyć współpracę z dostawcą usług płatniczych, który pomoże zorganizować bezpieczną przestrzeń dla handlu.

Pod kontrolą

Wiemy, że wdrażanie bezpiecznych rozwiązań płatniczych zawsze pociąga za sobą wiele pytań: czy moje dane są w dobrych rękach? Czy środki otrzymam na czas? Czy moja strona płatności będzie zawsze dostępna dla klientów? Właśnie dlatego dbamy o to, by nasza infrastruktura spełniała najwyższe standardy bezpieczeństwa, integralności i stabilności. Ponieważ znalezienie niezawodnej platformy płatniczej może być kłopotliwe, najlepiej wybrać taką, która łączy w sobie zarówno funkcje przetwarzania płatności, jak i skuteczną ochronę przed oszustwami.

Dla przykładu, Adyen w pełni opiera się na oprogramowaniu open source. Zapewnia to maksymalną kontrolę nad komponentami, jednocześnie gwarantując niezależność od wszelkich stron trzecich. Wszystkie działania związane z rozwojem, administrowaniem systemami, sieciami, zarządzaniem bazami danych i bezpieczeństwem przeprowadzane są we własnym zakresie, ponieważ ochrona danych klientów to podstawa działalności firmy.

Utrzymywanie procesu zakupu pod kontrolą i minimalizowanie ryzyka oszustw lub niepożądanych niebezpiecznych działań jest obowiązkiem sprzedawcy na każdym etapie przeprowadzania transakcji. By wszystko przebiegało sprawnie, powstał szereg rozwiązań, które pomagają w ograniczeniu najbardziej podatnych na zagrożenie punktów przetwarzania płatności. Właściciele biznesów, obecnie akceptujący transakcje na swojej stronie internetowej lub rozważający współpracę z agentem rozliczeniowym, prawdopodobnie słyszeli już o standardzie PCI.

Każda firma przyjmująca płatności kartą kredytową, musi stosować się do PCI DSS. Chociaż standard ten nie jest częścią żadnego prawa, jest używany na całym świecie. Payment Card Industry Data Security Standards (PCI DSS) to zbiór globalnych zasad bezpieczeństwa stworzonych w celu zapewnienia, że każde przedsiębiorstwo, które gromadzi, przetwarza, przechowuje lub przesyła dane właścicieli kart, utrzymuje bezpieczne środowisko ich informacji. PCI DSS ma zastosowanie do wszystkich podmiotów akceptujących karty kredytowe lub biorących udział w przetwarzaniu płatności, takich jak agenci rozliczeniowi, emitenci i dostawcy usług. Zgodność ze standardem

minimalizuje szanse na naruszenie danych w wyniku złośliwych ataków – jest zatem jednym z kroków, które właściciele biznesów powinni podjąć, by uodpornić się na wirtualne zagrożenia.

Zwiększyć bezpieczeństwo

W Adyen przetwarzamy płatności i przeprowadzamy kontrolę ryzyka w czasie krótszym niż sekunda, w zależności od szybkości działania zaangażowanego agenta rozliczeniowego lub emitenta. Ponieważ kwestia bezpieczeństwa klientów jest dla nas niezwykle ważna, zadbaliśmy o to, aby główne systemy były hostowane w oddzielnych centrach danych w Europie, Stanach Zjednoczonych i Australii. Nie zlecamy żadnej administracji stronom trzecim ani nie korzystamy z usług w chmurze publicznej do przetwarzania płatności. To także sposób na zwiększenie bezpieczeństwa wewnątrz firmy.

Wszystkie systemy są zbudowane w sposób zapewniający maksymalną redundancję. Moim zdaniem bardzo ważna jest również przejrzystość i uczciwość działania, zwłaszcza jeśli chodzi o dane i pieniądze. Jesteśmy głównym członkiem i licencjonowanym nabywcą kart Visa i MasterCard, a także przestrzegamy przepisów operacyjnych systemów kartowych i corocznych audytów naszych partnerów, m.in. Visa, MasterCard i banków, z którymi współpracujemy. Myślę, że jest to coś, co klienci doceniają. Na wartości zawsze zyskuje całościowa opieka nad procesem płatności. Dzięki temu firmy mogą usprawnić swoją działalność i zoptymalizować koszty.

> **Zagrażające bezpieczeństwu działania w sieci są zazwyczaj dokonywane dla osobistego zysku atakujących.**

Jest wiele czynników, które firma musi mieć na uwadze, gdy się rozwija, jednak bezpieczeństwo danych nie może być tym, który zostaje pominięty. Zapewnienie zgodności z przepisami na własną rękę nie jest jednak najłatwiejszym zadaniem. Z tego powodu wielu sprzedawców preferuje współpracę z dostawcami usług płatniczych, którzy zajmują się kwestiami PCI i oferują różne rozwiązania szyfrujące, by zapewnić odpowiedni poziom bezpieczeństwa płatności kartami. Jeśli moglibyśmy udzielić jakiejkolwiek porady w tym zakresie, należałoby upewnić się, że dany system jest zgodny ze standardami płatności, bezpieczeństwa i ryzykiem obowiązującym w kraju prowadzenia działalności, co obejmuje również metody płatności bez użycia kart.

Podejrzane działania i rosnąca liczba słabych punktów mogą zaszkodzić reputacji firmy i kosztować przedsiębiorstwa znacznie więcej niż pieniądze. Ruch na stronie i zgromadzone dane powinny być stale monitorowane i analizowane, by upewnić się, że nie utworzyły się żadne otwarte luki, które mogą zagrażać klientom. Należy uważnie obserwować wszelkiego rodzaju zagrożenia, ataki i podejrzane działania oraz niezwłocznie reagować w przypadku ich wystąpienia. Warto współpracować z wiarygodnymi firmami, które pomagają w przetwarzaniu płatności i utrzymywaniu bezpieczeństwa danych swoich klientów. Nie pozwalajmy nikomu myśleć, że nie jesteśmy gotowi na walkę ze złem.

Wpływ pandemii na automatyzację łańcucha dostaw

Wybuch pandemii koronawirusa znacząco zmienił rzeczywistość w wielu przedsiębiorstwach na całym świecie. Pracownicy korzystają z pracy zdalnej, telekonferencji, a spotkania twarzą w twarz zostały ograniczone do niezbędnego minimum. Wszechogarniająca automatyzacja, która na przestrzeni ostatnich kilku lat zredukowała liczbę osób pracujących na przykład na liniach montażowych, nie sprawiła jednak, że produkcja może być realizowana bez dostaw surowców.

Łukasz **Łukasiewicz**
Operations Manager,
SwipBox Polska

Globalność oraz skala koronawirusa już teraz odcisnęły swoje piętno na łańcuchu dostaw. Według prognoz między innymi ABI Research, światowe przychody z produkcji, które w tym roku miały wynieść 15 trylionów dolarów, w żaden sposób nawet nie zbliżą się do spodziewanego poziomu.

Automatyzacja czy cyfryzacja wpływa nie tylko na ograniczenie liczby pracowników, ale w wielu miejscach jej wprowadzenie jest związane bezpośrednio ze zwiększeniem ich efektywności. Systemy pracy w firmach logistycznych cały czas ewoluują. Robotyka jest bezapelacyjnym stymulatorem innowacyjności, który przyspiesza cyfrową transformację. Jej skutkiem jest ewolucja produktywności pracowników oraz powszechnie wiadoma oszczędność czasu w obszarze ich zaangażowania w mało wydajne działania.

Rosnące oczekiwania

Wymagania konsumentów sprawiły, że cyfryzacja stała się koniecznością. Potrzeby oraz oczekiwania nieustannie rosną, ponieważ odbiorcy oczekują przejrzystości czy całodobowego dostępu do informacji w zakresie potencjalnych przesunięć terminów dostaw. Automatyzacja ułatwia implementację nowatorskich modeli biznesowych, w które wpisują się łańcuchy dostaw jako kluczowe źródło satysfakcji klienta końcowego.

Sam proces automatyzacji łańcucha dostaw nie może zostać przeprowadzony w oderwaniu od innych wiodących działów przedsiębiorstwa, jak między innymi sprzedaż, IT czy human resources. Zarządzanie zmianą wymaga zaangażowania wszystkich działów, cele muszą zostać jasno określone, a optymalizacja kosztów usług nie powinna stanowić priorytetu samego w sobie.

Przyspieszenie procesów

Pandemia koronawirusa na wielu firmach logistycznych wymusiła przyspieszenie procesów, które mają pozwolić jeszcze skuteczniej realizować usługi, ale również przygotować się na to, co jeszcze niedawno wydawało się kompletną abstrakcją. W przypadku kolejnej „fali", która nie jest wykluczona, przedsiębiorstwa będą bazować na zdobytym już

doświadczeniu oraz działaniach, które przyniosły pozytywne efekty podczas kryzysu.

Sam wirus będzie mieć dla producentów konsekwencje na wielu płaszczyznach. Wystarczy wspomnieć o zabezpieczeniu dostaw czy przekrojowej analizie własnej działalności. Nowa rzeczywistość wymaga nowatorskich rozwiązań. Jednym z nich jest przyspieszona automatyzacja, która ma na celu dywersyfikację biznesu. Oczywiście, nie każdy podmiot może sobie na to pozwolić, lecz nieustanny rozwój sektora e-commerce wymaga odważnych decyzji nie tylko w obszarze cyfryzacji. Producenci dążą także do minimalizacji ryzyka związanego z łańcuchem dostaw. Coraz częściej pozyskują komponenty od jednego dostawcy, ale coraz rzadziej w tym samym miejscu. Im większy wachlarz potencjalnych opcji, tym większa szansa na zażegnanie kryzysu, otwarcie się na nowe możliwości oraz kontrolę samego łańcucha.

CZŁOWIEK NAJSŁABSZYM OGNIWEM – jak zminimalizować zagrożenia wynikające z ludzkich błędów w prowadzeniu przedsiębiorstwa?

Często spotkamy się ze stwierdzeniem, że człowiek jest najsłabszym ogniwem podczas pracy z systemami informatycznymi. Mimo to, według badania SAS przeprowadzonego w 2019 roku wśród 850 firm z regionu EMEA, ponad 43 proc. z nich, szukając nadużyć i błędów, opiera się jedynie na procesach manualnych – wykonywanych doraźnie przez pracowników.

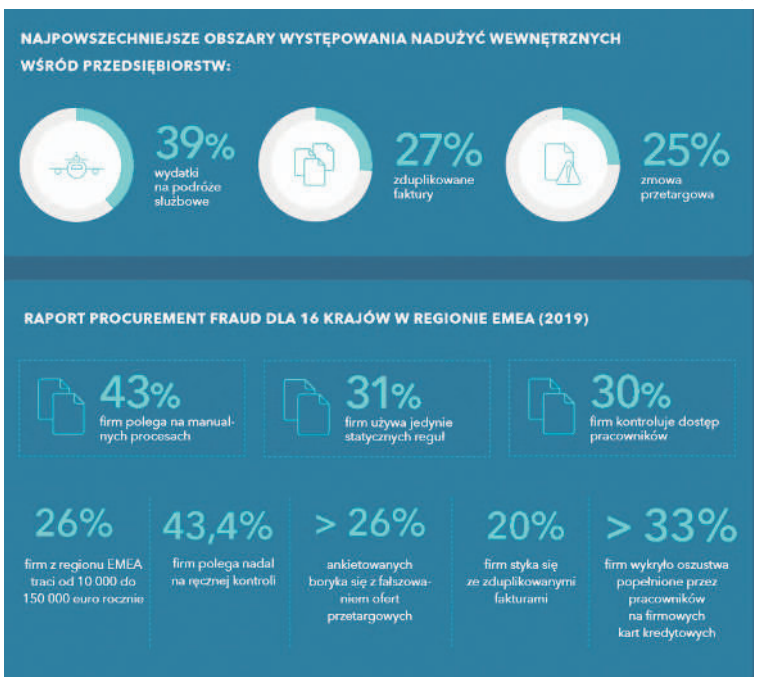
Agnieszka **Piechocka**
Customer Advisor, SAS

Człowiek nie jest najsłabszym ogniwem. Jest jednak ogniwem dużo bardziej podatnym na stres, nietypowe sytuacje i wrażliwym na czynniki zewnętrzne niż działające zawsze w ten sam sposób systemy. Widać to szczególnie w ostatnich tygodniach. Natłok informacji trudnych do zweryfikowania, dezorganizacja pracy firm, strach o zdrowie własne i bliskich, utrata pracy – to tylko niektóre czynniki sprzyjające popełnianiu nadużyć. Dokładając do tego chaos organizacyjny i braki kadrowe, naprawdę trudno jest uniknąć błędów.

Z jednej strony zwolnienia wymuszone obniżeniem przychodów firmy spowodowały konieczność przejęcia przez pozostałych pracowników nowych obowiązków. Z drugiej – wydłużone godziny pracy sklepów z artykułami pierwszej potrzeby wymagają zaangażowania większej liczby pracowników i zatrudniania nowych osób w trybie natychmiastowym, czasem nawet bez sprawdzania ich tożsamości. A podjęcie współpracy z osobą lub firmą bez uprzedniego sprawdzenia jej wiarygodności może nieść za sobą opłakane skutki.

Nadużycia wewnętrznym problemem organizacji

Nadużycia wewnętrzne mogą pojawić się w każdej organizacji w wyniku zaniedbania procesów monitorujących nieprawidłowe działania. Mogą wynikać zarówno z błędów, jak i celowego działania nastawionego na osiągnięcie zysku. Podczas gdy nadużycia postrzega się głównie jako zewnętrzne zagrożenie, w połowie przypadków mają udział pracownicy. Szczegółowe informacje dotyczące skali problemu można znaleźć na załączonej grafice.



W tej sytuacji warto zwrócić się w kierunku zautomatyzowanych systemów analitycznych opartych o algorytmy sztucznej inteligencji jako narzędzia do walki z możliwymi nadużyciami.

Istnieje szereg dobrych praktyk i procesów, których wdrożenie przyczynia się do zmniejszenia strat. Działania proaktywne (m.in. szkolenie pracowników) i reaktywne (m.in. szukanie nietypowego zachowania w danych historycznych) są tak samo ważne, aby zdawać sobie sprawę ze schematów zdarzeń powodujących straty. Nie mniej istotna jest analiza znanych już rodzajów nadużyć, aby skutecznie im zapobiegać.

Analityka hybrydowa bronią przeciw nadużyciom

Zmieniające się trendy dotyczące nadużyć wymagają zastosowania narzędzi sprawnie dostosowujących się do nowych warunków biznesowych. Stosowanie analityki hybrydowej umożliwia pracę na wielu poziomach, co jest bardziej efektywne ze względu na połączenie wiedzy eksperckiej wraz z metodami uczenia maszynowego, pozwalającymi na znalezienie w danych nieznanych wzorców zachowania. Dodatkowo dołączenie sieci wzbogaca algorytmy o informacje o zorganizowanych działaniach i ukrytych powiązaniach.

Wśród metod analityki hybrydowej gwarantujących najlepszą efektywność warto wymienić:

- łączenie baz danych i rejestrów z różnych źródeł,
- zautomatyzowane reguły biznesowe aplikujące wiedzę ekspercką,
- analizę sieci powiązań,
- analizę tekstu (artykułów prasowych i notatek pracowniczych),
- wykrywanie anomalii,
- modelowanie predykcyjne (wykrywanie nieznanych wzorców zachowań na podstawie historycznych przypadków).

Nie ma jednego dobrego rozwiązania, aby zapobiec wszystkim błędom i nadużyciom. Jednak dzięki połączeniu różnych źródeł danych i metod analityki hybrydowej na platformie SAS Viya, możliwe staje się minimalizowanie błędów ludzkich i jednocześnie odzyskanie pieniędzy traconych na nadużyciach.

Trzy drogi do tego, aby zdalna praca była szeroko dostępna i bezpieczna

Pandemia COVID-19 powoduje powszechne zakłócenia, w związku z czym rządy w wielu krajach zwróciły się do przedsiębiorców z prośbą o umożliwienie pracownikom wykonywania pracy zdalnie. Polskie firmy pozytywnie zareagowały na prośby i wiele przedsiębiorstw wdrożyło elastyczne formy pracy i pracę zdalną, aby zminimalizować ryzyko zarażenia wśród swoich pracowników.

Anthony **Spiteri**,
Joseph **Chan**

Veeam Software

Łatwość wdrożenia tego typu działań jest możliwa dzięki nowoczesnym rozwiązaniom, jak choćby chmura obliczeniowa. To właśnie ona jest kluczowym czynnikiem umożliwiającym efektywną pracę zdalną i gwarantującym jej sukces. Chmura umożliwia pracownikom współpracę, udostępnianie i dostęp do wszelkich plików i dokumentów w dowolnym miejscu i czasie. Według firmy Gartner, do 2022 r. nawet 60 proc. organizacji będzie korzystać z oferty usług zarządzanych w chmurze oferowanych przez zewnętrznego dostawcę usług. Wymaga to jednak skupienia się na trzech kluczowych obszarach, które zapewnią przedsiębiorcom możliwość łatwego przestawienia się na pracę zdalną bez zakłóceń dla danych i z zachowaniem pełnego ich bezpieczeństwa.

Rozwój cloud data managment

Łatwy dostęp do danych jest kluczem do zdalnej pracy, a cloud data managment jest rozwiązaniem, które najlepiej wspiera tę formę wykonywania obowiązków służbowych. Przy wdrażaniu rozwiązań chmurowych należy jednak bezwzględnie pamiętać o ochronie danych, zwłaszcza że w ostatnich latach byliśmy świadkami wielu naruszeń ich bezpieczeństwa. Po roku 2020 spodziewamy się wyraźnego zwiększenia mobilności i możliwości przenoszenia danych w ramach zarządzania danymi w chmurze (CDM), co jednocześnie musi się wiązać z wprowadzeniem dodatkowych środków bezpieczeństwa. Firmy chcą zwiększyć dostępność danych w zdalnym miejscu pracy, jednocześnie dużo uwagi poświęcając odpowiedniemu ich zabezpieczeniu – zarówno pod kątem ryzyka ich utraty, możliwości łatwego odtworzenia, jak również zapewnienia ciągłości działania przedsiębiorstwa. Prognozujemy, że znaczenie CDM wzrośnie już w przyszłym roku, gdy łatwe, dostępne i bezpieczne dane staną się niezbędne dla codziennego funkcjonowania firm.

Ciągłe tworzenie kopii zapasowych może przyspieszyć transformację

Przedsiębiorstwa muszą mieć świadomość optymalnych sposobów obchodzenia się z danymi w chmurach i wykorzystywać lepsze narzędzia do tworzenia ich kopii zapasowych. Zgodnie z raportem Veeam 2019 Cloud Data Management już prawie jedna trzecia firm stale tworzy kopie zapasowe i replikuje aplikacje o wysokim priorytecie. Liczba ta będzie rosnąć, ponieważ coraz więcej firm dostrzega znaczenie łatwego odzyskiwania swoich krytycznych danych.

– Praca zdalna niesie ze sobą więcej zagrożeń dla danych niż ta wykonywana w siedzibie przedsiębiorcy. Wymaga ona nie tylko odpowiedniego zabezpieczenia wykorzystywanego sprzętu przed dostępem nieuprawionych osób czy bezpiecznych łącz. To także dbałość o bezpieczeństwo firmowych danych i ochrona przed ich utratą. Nasze badania pokazały, że za utratę danych w zdecydowanej większości odpowiada błąd ludzki. Ktoś przypadkowo skasuje ważny folder, ktoś usunie bazę danych myśląc, że usuwa ją jedynie z własnego komputera – takich przypadków jest naprawdę sporo. Oznacza to wprost, że praca zdalna wymaga wdrożenia odpowiednich narzędzi, które dbają o bezpieczeństwo firmowych danych i potrafią je odtworzyć niemal natychmiast, niezależnie, czy błąd popełnił pracownik, zawiódł sprzęt czy firma stała się celem ataku hakerskiego – komentuje Tomasz Krajewski, Technical Senior Director w Veeam Software.

W tym dziesięcioleciu wzrośnie również liczba platform i narzędzi, dzięki którym firmy będą mogły w sposób ciągły tworzyć kopie zapasowe swoich danych w wielu środowiskach i w ciągu kilku minut odzyskiwać je w całości. Te same narzędzia mogą również zapewnić przedsiębiorstwom szczegółową analizę zbiorów danych, pomagając im w podejmowaniu świadomych decyzji w zakresie transformacji cyfrowej i strategii rozwoju działalności gospodarczej.

Przyjęcie różnych sposobów automatyzacji

W związku z tym, że świat wciąż domaga się coraz większej wydajności pracy, będziemy świadkami zwiększonej automatyzacji w obszarach zadań i procesów w organizacjach wszędzie tam, gdzie da się zastąpić powtarzalne zadania wykonywane obecnie przez ludzi. Jednym z ważnych przykładów jest Infrastruktura Jako Kod (IaC). Automatyzacja infrastruktury, podobnie jak IaC, pozwala organizacjom na skonfigurowanie kompletnej infrastruktury za pomocą skryptu przy jednoczesnym odejściu od ręcznej konfiguracji.

Chociaż automatyzacja nie jest czymś, co jest nowe, to wkrótce okaże się, że ci, którzy już ją wdrożyli, przechodzą na kombinacje różnych jej typów, w tym IaC. Dzięki temu firmy mogą skupić się na ważniejszych projektach. Nigdy nie jesteśmy w stanie przewidzieć globalnych kryzysów, katastrof naturalnych i problemów, które jak ten obecny rzutują na formę pracy w wielu krajach. Jednakże odpowiednia technologia może nam pomóc w odpowiednim przygotowaniu firmy do działania w niestandardowych warunkach i otoczeniu biznesowym.

Reakcja firm na COVID-19 stanowi doskonały przykład na to, jak przedsiębiorstwa mogą zachować ciągłość działania dzięki innowacjom technologicznym. Umożliwiając pracownikom pracę zdalną, minimalizują oni również zagrożenia dla zdrowia i uwalniają ich od ograniczeń lokalizacyjnych i czasowych.

Gdyby nie chmura obliczeniowa, firmy byłyby teraz w jeszcze większych tarapatach

COVID-19 wyrządził ogromne spustoszenia w globalnej gospodarce, a jesteśmy dopiero na początku liczenia strat. Dewastacyjny wpływ pandemii na gospodarkę byłby z pewnością jeszcze gorszy, gdyby nie przejście wielu firm i instytucji na model pracy zdalnej, który był możliwy dzięki wcześniejszym lub podejmowanym na szybko inwestycjom w chmurę obliczeniową.

Andrzej **Stella-Sawicki**

wiceprezes i dyrektor operacyjny, CloudFerro

Wpływ koronawirusa bez wątpienia jest katastrofalny ze społecznego i gospodarczego punktu widzenia. Jednak z pewnością byłby on znacznie poważniejszy, gdyby nie inwestycje przedsiębiorstw w cloud computing. Choć przed pandemią w Polsce z chmury korzystało kilkanaście procent przedsiębiorstw; nawet tak niskie zaangażowanie polskich firm należy ocenić pozytywnie, jako dobrą bazę teraźniejszych i przyszłych transformacji. Chmura obliczeniowa zasila dzisiaj niemal wszystko to, co pozwala nam w miarę normalnie funkcjonować w czasach izolacji. Praca zdalna, dostęp do filmów i seriali przez platformy typu Netflix, dostęp do książek z poziomu np. aplikacji Storytel, automatyzacja łańcuchów dostaw sieci retailowych czy po prostu działanie aplikacji zakupowych – to zasługa chmury.

Bohater nieoczekiwanej rewolucji

Na zachodzie od dawna dostrzegano wartość chmury. Według firmy analitycznej Canalys, w 2019 roku organizacje wydały rekordową sumę 107 mld dolarów na wdrożenia lub rozwój infrastruktury chmurowej i było to aż o 37 proc. więcej niż w roku poprzednim. Natomiast Gartner przewiduje, że światowe wydatki na usługi chmury publicznej wzrosną w 2020 roku o 17 proc., do kwoty ponad 266 mld dolarów.

Szybkie tempo adopcji chmury

To, że dziś firmy korzystające z cloud computingu mogą kontynuować wszystkie lub większość dotychczasowych procesów, zawdzięczają w dużej mierze wcześniejszym inwestycjom w rozwiązania cloudowe. To wszystko nie byłoby możliwe, gdyby nie naprawdę szybkie tempo adopcji chmury. Jeszcze kilka lat temu firmom brakowało narzędzi, aby umożliwić pracownikom natychmiastowe przejście na pracę zdalną. Dziś firmy mają właściwie wszystko, czego potrzebują, aby pracownicy mogli wykonywać swoje zadania z domu – szybki Internet, przystępne cenowo komputery osobiste, systemy zabezpieczeń w formie zaawansowanych sposobów rejestracji i uwierzytelniania oraz dostępność większości systemów biznesowych w chmurze. Okazuje się, że chmura obliczeniowa w obliczu dzisiejszego ogromnego wyzwania dobrze spełnia swoją rolę, zapewniając platformę do pracy zdalnej, współdzielenie dokumentów, możliwość szybkiego skalowania zasobów. Na przykładzie naszej organizacji – od momentu ogłoszenia pandemii dostosowaliśmy model działania przechodząc na pracę zdalną, ale dzięki rozwiązaniom chmurowym nasi klienci nie odczuli żadnej zmiany w jakości świadczonych przez nas usług.

Zmiana na stałe

Co więcej, wydaje się, że ta nagła rewolucja może na stałe zmienić system, w którym funkcjonujemy, pracujemy czy uczymy się. W przyszłości, nawet jak już wrócimy do normalności, pracodawcy, pracownicy, nauczyciele, studenci i uczniowie, dostrzegając zalety pracy zdalnej, z pewnością będą z nich korzystać na szerszą skalę. Gdyby taka sytuacja wydarzyła się dekadę wcześniej, IT byłoby w zupełnie innej sytuacji. Według badań przeprowadzonych przez kierownictwo działu IT firmy Osterman Research, w 2010 roku przeciętna firma wydawała rocznie na przetwarzanie w chmurze zaledwie 6300 dolarów rocznie, co w przeliczeniu na jednego pracownika wynosiło nieco ponad 23 dolary. To niewielki ułamek obecnych nakładów na ten obszar IT.