15 listopada 2023, nr 11
www.crn.pl
ISSN 2080-8607

CRN

25 LAT CRN POLSKA

Raport CRN
Infrastruktura w modelu usługowym

Wacław Iszkowski
Potrzebny system cyberkontrataków

Canalys Forum
AI w kanale partnerskim

Maciej Filipkowski
Efekt Ringelmanna

XChange EMEA
Cybersecurity i networking

Okiem użytkownika
Cyfryzacja Białowieskiego Parku Narodowego

Sztuka ZARZĄDZANIA DANYMI

„Zasada GIGO nie straciła nic ze swej istotności”
– Tomasz Nitsch, prezes DAMA Poland Chapter i CDO Banku Millennium

Bezpieczeństwo urządzeń końcowych | Programy partnerskie | Monitoring wydajności aplikacji

Cyberbezpieczeństwo: koniec obietnic, czas na dowody
Nowoczesne narzędzia otwierają nowe możliwości w zakresie zabezpieczania sprzętu, ale niosą też ze sobą pewne wyzwania.

22

Infrastruktura w modelu usługowym: czy i kiedy?
Przez ostatnich kilkanaście lat usługi chmury publicznej ugruntowały swoją pozycję na cyfrowym rynku. Obecnie dla klientów oczywiste są zarówno wady, jak też zalety tego modelu dostarczania zasobów oraz płynące z niego czynniki ryzyka.

42

54

Efekt Ringelmanna, czyli małe jest piękne
Wciąż spotyka się menedżerów i przedsiębiorców, którzy uważają, że im więcej osób uczestniczy w danym projekcie, tym szybciej zostanie on ukończony. To błąd.

SPIS TREŚCI

8 **Targi it-sa**
Norymberga w pierwszej połowie października zamienia się w europejską stolicę cyberbezpieczeństwa

11 **Rising Stars of Cybersecurity: NIS2 na horyzoncie**
Relacja z 3. edycji konferencji organizowanej przez Dagma Bezpieczeństwo IT

12 **Canalys Forum EMEA: ruszyła gorączka złota**
Analitycy Canalysu są przekonani, że sztuczna inteligencja nie przeminie jako kolejny „buzzword", ale w znaczący sposób wpłynie na krajobraz kanału sprzedaży IT

14 **Czas przełomu w ekosystemie partnerskim**
Za kilka kwartałów większość kupujących w sektorze IT to będą milenialsi – mówi Jay McBain, Chief Analyst w Canalysie, w rozmowie z CRN Polska

15 **Rynek chipów powraca do zdrowia**
Segment półprzewodników będzie rozwijać się w szybkim tempie

16 **CRN XChange EMEA z polskimi akcentami**
Zorganizowany przez brytyjską redakcję CRN-a zjazd producentów, dystrybutorów i integratorów z regionu EMEA poświęcony był działaniom M&A, ale także sektorowi cyberbezpieczeństwa

18 **Zarządzanie danymi, czyli trudna sztuka wyboru rzeczy ważnych**
Rozmowa z Tomaszem Nitschem, Chief Data Officerem w Banku Millenium oraz prezesem zarządu DAMA Poland Chapter, organizacji zrzeszającej profesjonalistów zajmujących się danymi

22 **Cyberbezpieczeństwo: koniec obietnic, czas na dowody**
W segmencie produktów do ochrony urządzeń końcowych zaszły istotne zmiany

30 **Chmura i usługi w programach partnerskich**
Model usługowy wymusza zmianę benefitów, szkoleń, modelu rozliczeniowego, a nawet statusów partnerskich

33 **Koniec ze skostniałymi programami partnerskimi**
Rozmowa z Marcinem Gwarą, Channel Managerem w Fujitsu

35 **Obserwowalność: nowe, modne słowo?**
Działy IT coraz częściej sięgają po Application Performance Monitoring

38 **Nastawienie do usług powinno się zmienić**
Rozmowa z Mariuszem Rzepką, Development Directorem of MSP & Cybersecurity Services w CEEcloud

42 **Infrastruktura w modelu usługowym: czy i kiedy?**
Zaawansowane rozwiązania infrastrukturalne w formie usługi rozliczanej abonamentowo, w niektórych krajach przyjęły się nadspodziewanie dobrze, ale w Polsce jeszcze na nie za wcześnie

46 **Usługi cyberbezpieczeństwa: ostatnia deska ratunku**
Nakłady ponoszone przez firmy na systemy bezpieczeństwa IT są niewspółmierne do osiąganych rezultatów

51 **Nie od razu AI zbudowano**
Felieton Larry'ego Walsha

52 **Wykorzystanie AI w rekrutacji**
Rozmowa z Tomaszem Millerem, IT Managing Consultantem w Yard Corporate

54 **Efekt Ringelmanna, czyli małe jest piękne**
Liczebność zespołu a efektywność działania

56 **Czy i jak wspierać pracowników w kryzysie?**
Bez względu na to, co jest źródłem kryzysu pracownika, objawy na zewnątrz będą podobne

58 **Po co nam komisja europejska?**
Felieton Jerzego Martini

59 **Decoupling po amerykańsku**
Felieton Arnolda Adamczyka

60 **Dane dobre z natury**
Rozmowa z Katarzyną Kopiejczyk, zastępcą dyrektora ds. administracyjnych w Białowieskim Parku Narodowym

64 **O trendach w branży teleinformatycznej**
Felieton Wacława Iszkowskiego

66 **Europa jest liderem**
Felieton Wojciecha Urbanka

Fot. Adobe Stock

Interes **do zrobienia**

Interes? A ile można stracić?". „Co się mnie pytasz, ile można stracić! Się mnie natychmiast zapytujesz, ile można zarobić!". „Ile się zarobi, to się zarobi. Ja się pytam: ile trzeba mieć, żeby ryzykować w razie, że się straci?".

Przytoczony dialog jest bezsprzecznie kultowy dla wszystkich miłośników kabaretowych szmoncesów. Sęk w tym, że w druku traci on większość ze swego uroku, ale za to zachowuje wszelkie atrybuty tak zwanej życiowej mądrości. Chociażby takiej, jaką wykazała się pewna staruszka, która w czasach słusznie minionych przyjechała PKS-em z prowincji do stolicy, żeby załatwić jakąś urzędową sprawę. Następnie musiała tłoczyć się razem z innymi pasażerami w autobusie linii 116, próbując dotrzeć na Żoliborz. Na przystanku przy Miodowej kierowca powiedział, że dalej nie jedzie, bo przednim pomostem pchał się jakiś facet w bereciku i drzwi się nie zamykały. Więc wszyscy zaczęli faceta błagać, żeby dał ludziom żyć i wysiadł, ale on nic i widać było, że nie ustąpi. I wtedy staruszka wykrzyczała złotą myśl: „Berecik! Zrućta mu ludzie berecik!". Ktoś mu ten berecik zdjął, rzucił na chodnik i on bez słowa wyskoczył. Drzwi się zamknęły i autobus pojechał (copyright: Janusz Głowacki, „Z głowy").

Oni tylko niosą pomoc.

No więc – i tu przechodzę do rzeczy – kiedy rosnący odsetek społeczeństw europejskich martwi się rosnącymi kosztami życia w związku z regulacjami dotyczącymi zrównoważonego rozwoju, mnie wspomniana już tak zwana życiowa mądrość podpowiada, że... jest interes do zrobienia. Co by się zgadzało z raportem Canalysa, z którego wynika, że 40 proc. przedsiębiorców nie sprosta wyśrubowanym środowiskowym normom UE. Z drugiej strony ponad 50 proc. integratorów IT z naszego regionu deklaruje, że już w tym roku wygeneruje mniejsze bądź większe przychody na wdrażaniu rozwiązań IT, które mają pomóc wspomnianym wcześniej przedsiębiorcom w uzyskaniu pożądanej zgodności. Co niejako potwierdza tezę, jaką postawiłem jakiś czas temu porównując regulacje ESG ze słynnym RODO, które to rozporządzenie dało szeroko rozumianemu biznesowi do wiwatu, za to część dostawców IT pomogła związany z tym ból głowy uleczyć, zamieniając go przy tym na przychody.

Tym samym nie jest do końca prawdą, że – jak mówił podczas debaty w Warsaw Enterprise Institute prof. Waldemar Rogowski ze Szkoły Głównej Handlowej – „inicjatorami dyskusji i ‘namawiaczami' do ESG są sektory doradztwa biznesowego i audytu, które w krótkim okresie będą beneficjentami wdrożenia raportowania ESG". Ja bym uzupełnił tę opinię o niektórych dostawców ISV oraz integratorów IT. Z takim jednak zastrzeżeniem, że ci akurat nikogo do tego nie namawiają. Oni tylko niosą pomoc.

Tomasz Gołębiowski
Redaktor naczelny

CRN

MIESIĘCZNIK CRN POLSKA
www.CRN.pl

Rok 26, numer 11 (493), 15 listopada 2023
PL ISSN 2080-8607

REDAKCJA
Aleja Stanów Zjednoczonych 51, lok. 508
04-028 Warszawa
redakcja@crn.pl

Tomasz Gołębiowski **tg**
(redaktor naczelny)
tel. 608 425 699
tomasz.golebiowski@crn.pl

Wojciech Urbanek **wu**
(zastępca red. naczelnego)
tel. 691 672 065
wojciech.urbanek@crn.pl

Karolina Marszałek **km**
(sekretarz redakcji)
karolina.marszalek@crn.pl

Andrzej Gontarz **ag**
andrzej.gontarz@crn.pl

Krzysztof Jakubik **kj**
krzysztof.jakubik@crn.pl

Krzysztof Pasławski **kp**
krzysztof.paslawski@crn.pl

Tomasz Janoś **tj**
tomasz.janos@crn.pl

FELIETONY
Arnold Adamczyk, Wacław Iszkowski, Jerzy Martini, Wojciech Urbanek, Larry Walsh

GRAFIKA, LAYOUT, KOORDYNACJA PRODUKCJI:
Tomasz Baziuk

FOTOGRAFIE
Theta Art Studio Tomasz Pisiński, PhotobyMysluk.pl, Adrian Stykowski, Piotr Syndoman, archiwum

PRENUMERATA
prenumerata@crn.pl

REKLAMA I PROJEKTY SPECJALNE
Agata Myśluk
tel. 694 455 426
agata.mysluk@crn.pl

Jacek Goszczycki
tel. 601 935 513
jacek.goszczycki@crn.pl

WYDAWCA
PERISTERI MEDIA COMPANY
Peristeri Sp. z o.o.
Aleja Stanów Zjednoczonych 51, lok. 508
04-028 Warszawa

Od ćwierć wieku relacjonujemy najważniejsze wydarzenia w kanale sprzedaży IT. Zaczęliśmy w czasie, kiedy działalność prowadziło w Polsce ponad 250 (!) dystrybutorów i subdystrybutorów, chmura była zjawiskiem atmosferycznym, Bill Gates zamiast ratować świat naprawiał Windowsa, a Elon Musk negocjował z szefami Compaqa sprzedaż Zip2. Krótko mówiąc, to były stare dobre czasy, a poniżej garść wspomnień z naszego polskiego „podwórka".

25 LAT CRN POLSKA

Kwiecień 2002

Prezesem polskiego oddziału Panasonica została Wiesława Wasilewska, która tym samym jest pierwszą kobietą na świecie, która stanęła na czele handlowego oddziału koncernu (Matsushita Electric Industrial) i jednocześnie pierwszą Polką na stanowisku prezesa polskiego oddziału. Nominacja ta wynika z nowej strategii działania firmy, której głównym założeniem jest wzrost liczby miejscowych managerów na głównych stanowiskach w europejskich oddziałach japońskiego koncernu. Wiesława Wasilewska rozpoczęła pracę dla Panasonica w chwili powstania polskiego oddziału, a więc w 1993 r. Utworzyła pierwszą strukturę sprzedaży produktów Panasonic i Technics.

Od redakcji

Wiesława Wasilewska pełniła swoją zaszczytną rolę przez kolejnych pięć lat, po czym odeszła na emeryturę. Nie stała się postacią legendarną w branży elektronicznej, gdyż przez dłuższy czas zajmowała się w japońskim koncernie sprzedażą żywności, produktów chemicznych i tekstyliów. Dopiero z czasem Japończycy wprowadzili do Polski sprzęt Panasonica i Technicsa, z myślą o sprzedaży ich w sieci Peweksu. A skoro już padła ta nazwa (młodsi czytelnicy niech sobie ją wyguglują), to już wiadomo, że kariera pani Wiesławy rozkręcała się w latach 80. Radziła sobie świetnie, awansując od funkcji handlowca, przez kolejne szczeble aż do fotela prezesa. Co dwie dekady temu w branży elektronicznej było dla kobiety osiągnięciem wyjątkowym, a jeśli chodzi o koncerny japońskie, porównywalnym z górskimi wyczynami Wandy Rutkiewicz.

Maj 2002

Dotrzymywanie terminów dostaw, ceny i czas realizacji zamówienia – to według ostatniego badania Channel Track 2001 najważniejsze kryteria, którymi kierują się resellerzy, wybierając dystrybutora. Na liście kryteriów (w ankiecie było ich 17), którymi resellerzy kierowali się przy wyborze dostawcy znalazły się ponadto: dostępność produktów z cennika w magazynie i serwis gwarancyjny. Sprawa więc na pozór jest prosta. Jeśli dystrybutor chce zdobyć i utrzymać klientów, powinien położyć szczególny nacisk właśnie na te aspekty współpracy z nimi.

Od redakcji

Pewne rzeczy są niezmienne i to, co liczyło się dla partnerów ponad dwie dekady temu, ma znaczenie również obecnie. Nie da się prowadzić udanej działalności dystrybucyjnej nie dotrzymując terminów dostaw lub bez towaru na magazynie. A co w takim razie decyduje o długofalowym sukcesie producentów, w kontekście ich współpracy z kanałem partnerskim? Mamy dobrą wiadomość: w tym roku, po raz pierwszy w polskim kanale sprzedaży IT ruszył program certyfikacji vendorów. Odbywa się ona według kryteriów ustalonych przez integratorów, którzy wskazali, jakie usługi są dla nich kluczowe we współpracy z producentami. Wyniki procedury certyfikacji, wraz z pełnym jej opisem, ogłosimy już w grudniu tego roku!

Czerwiec 2002

Dell ma znakomity model działania wsparty nowoczesnymi technologiami. Jaka inna światowa firma osiąga około 50 proc. obrotów przez internet? Czyż nie jest to najbardziej efektywny sposób docierania do małych i średnich firm? Dzięki temu nie muszę klienta obciążać kosztami związanymi z kanałem partnerskim. Przy czym nie odmawiamy resellerom współpracy przy ciekawych projektach. Jednak i bez rozbudowanego kanału partnerskiego zajmujemy pierwszą pozycję na świecie pod względem sprzedaży sprzętu PC – podkreślał Roman Durka.

Od redakcji

Rozbudowa portfolio Della w stronę zaawansowanych rozwiązań IT nie postawiła przed firmą z Austin wyboru: sukces na rynku sprzętowych wdrożeń informatycznych w firmach i instytucjach gwarantują zaangażowani, profesjonalni integratorzy. Niedawno braliśmy udział w rozmowie z Diego Majdalanim, szefem światowego kanału partnerskiego Della, który na pytanie: dlaczego dopiero teraz producent wprowadził w życie strategię Partner First w segmencie storage'u, odpowiedział: „zawsze wiedzieliśmy, że z partnerami osiągniemy więcej, ale zajęło nam sporo czasu wdrożenie tego w życie". Nic dodać, nic ująć.

MIESIĄC

na plusie

Huawei po okresie sporego spadku sprzedaży i rentowności wskutek amerykańskich sankcji zaczyna wracać do formy. Po trzech kwartałach 2023 r. koncern osiągnął przychody w wysokości 456,6 mld juanów (62,5 mld dol.), co oznacza wzrost o 2,4 proc. rok do roku w chińskiej walucie. W tym czasie marża zysku netto wyniosła 16 proc. (73,06 mld juanów, tj. 10 mld dol.). To blisko trzykrotna poprawa rentowności rok do roku.

Amazon Web Services w III kw. 2023 r. zanotowało 12-procentowy wzrost sprzedaży rok do roku, do poziomu 23,1 mld dol. Taką samą dynamikę wykazały obroty AWS-u w poprzednim kwartale (+12 proc., 22,1 mld dol.), co oznacza koniec spadków w ujęciu kwartał do kwartału. Przy czym zysk operacyjny poprawił się o 30 proc. rok do roku, do poziomu 7 mld dol. Niemniej CEO Amazona Andy Jassy przyznaje, że klienci nadal ostrożnie podchodzą do wydatków. Spodziewa się natomiast, że z korzyścią dla partnerów wznowią projekty migracji obciążeń lokalnych do chmury, które utknęły w 2023 r.

Sygnity w III kw. 2023 r. (IV kw. roku obrotowego 2022/2023) uzyskało skonsolidowany zysk netto w wysokości 9 mln zł, podczas gdy przed rokiem było to 4,4 mln zł. Wyższa była także wartość sprzedaży, która według wstępnych wyliczeń wyniosła 59,2 mln zł (rok wcześniej było to 51,7 mln zł). Ostateczne wyniki finansowe za omawiany okres mają zostać przedstawione niebawem w raporcie za IV kwartał roku obrotowego 2022/2023.

Microsoft w III kw. br. (czyli w swoim I kw. 2024) zwiększył przychody o 13 proc., do poziomu 56,5 mld dol., a zysk netto o 27 proc., do 22,3 mld dol. Do poprawy bilansu w br. istotnie przyczyniła się wysoka sprzedaż w segmencie chmurowym. Microsoft Cloud przyniósł 31,8 mld dol. obrotu, co oznacza wzrost o 23 proc. rok do roku. W segmencie inteligentnej chmury przychody wyniosły 24,3 mld dol. (+19 proc. r/r). Przychody z Azure i innych usług w chmurze zwiększyły się o 28 proc. r/r. Stało za tym m.in. większe niż oczekiwano wykorzystanie mocy obliczeniowej przez usługi AI. Koncern donosi także o dużym zainteresowaniu nowym asystentem AI M365 Copilot.

Jensen Huang, CEO Nvidii jest najlepiej postrzeganym przez pracowników liderem biznesowym – wynika z ankiety przeprowadzonej na platformie Blind, sieci społecznościowej profesjonalistów. Aż 96 proc. pracowników pochwala jego zarządzanie korporacją, a tylko 3 proc. wyraziło dezaprobatę (pozostali nie mieli zdania). Na drugiej pozycji uplasował się szef Walmarta, a na trzeciej Nikesh Arora, CEO Palo Alto Networks (84 proc. akceptacji, 9 proc. niezadowolonych). Jeśli chodzi o pozostałych liderów dużych firm IT, to wysoko uplasowali się również Pat Gelsinger, szef Intela (54 proc.) – 18 pozycja w ogólnym rankingu i szef Cisco Chuck Robbins (49 proc.) – 24 miejsce.

na minusie

SolarWinds znalazło się pod ostrzałem Amerykańskiej Komisji Papierów Wartościowych i Giełd. Urzędnicy SEC zarzucają producentowi oprogramowania i jego dyrektorowi ds. bezpieczeństwa informacji, Timowi Brownowi, że „oszukali inwestorów i klientów poprzez fałszywe oświadczenia, zaniechania i schematy, ukrywające zarówno złe praktyki spółki w zakresie cyberbezpieczeństwa, jak i zwiększone – i rosnące – ryzyko cyberbezpieczeństwa" – informuje redakcja CRN USA. SEC wskazuje w tym kontekście na okres od grudnia 2018 r. do stycznia 2021 r. Według SEC dostawca ignorował ostrzeżenia o lukach w zabezpieczeniach. SolarWinds nie zgadza się z zarzutami SEC.

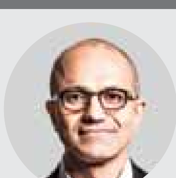
Intel kolejny kwartał z rzędu odnotował spadek rentowności w ujęciu rok do roku. Zysk netto stopniał o 70 proc., do 297 mln dol. (0,41 dol. na akcję non-GAAP), przy przychodach mniejszych o 8 proc. r/r (14,2 mld dol.). To jednak mimo wszystko bilans dużo lepszy, niż spodziewali się analitycy (średnio 0,22 dol. zysku na akcję i 13,6 mld dol. sprzedaży). Intel przekroczył ponadto własną prognozę z czerwca br.

Komenda Główna Policja musiała unieważnić ogłoszone w sierpniu br. postępowanie na zawarcie umowy ramowej na dostawę sprzętu drukującego i skanerów. Zdaniem KGP przetarg obarczony jest niemożliwą do usunięcia wadą, która nie pozwala na zawarcie niepodlegającej unieważnieniu umowy (art. 255 pkt. 6 Prawa zamówień publicznych). W uzasadnieniu stwierdzono, że zamawiający nie opublikował odpowiedzi na wnioski o wyjaśnienie treści SWZ, które zostały złożone w odpowiednim terminie przed upływem czasu na składanie ofert (który minął 26.10.2023 o godz. 9.30). Brak odpowiedzi stanowi naruszenie art. 135 ust. 2 Prawa zamówień publicznych.

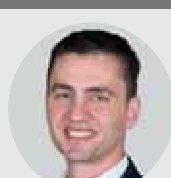
Negocjacje w sprawie fuzji pomiędzy Western Digital i Kioxią zostały odwołane – twierdzi japoński serwis Nikkei. Stało się to wkrótce po tym, jak SK Hynix, który ma 15 proc. udziału w Kioxii, sprzeciwił się połączeniu, uzasadniając, że nie leży ono w interesie akcjonariuszy. Kim Woo-hyun, dyrektor finansowy koreańskiego producenta DRAM i NAND flash, twierdzi przy tym, że nie może ujawnić konkretnych powodów sprzeciwu, ze względu na umowy o poufności.

Polska spadła na 18 miejsce (spośród 66) pod względem warunków do pracy zdalnej, o 5 miejsc niżej niż w 2022 r. – wynika z badania przeprowadzonego przez NordLayer. Nasz kraj został znacznie wyżej sklasyfikowany (8 miejsce) pod względem bezpieczeństwa cybernetycznego, wykazując się najwyższej klasy zdolnością reagowania (1 miejsce) i rygorystycznymi środkami prawnymi (6). Ogólnie pod względem infrastruktury cyfrowej i fizycznej Polska zajmuje dopiero 36 miejsce, przez słabą jakość Internetu (33 pozycja) i e-infrastruktury (45).

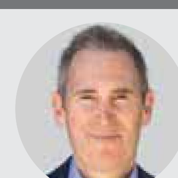
powiedzieli



„Jesteśmy bardzo zadowoleni, że coś zupełnie nowego cieszy się takim poziomem ekscytacji" **– Satya Nadella, CEO Microsoftu o M365 Copilot.**



„Zagrożeniu cyberatakami można zaradzić jedynie poprzez wspólne działania firm" **– Danny Allan, dyrektor ds. technicznych Veeam.**



„Jest to już dość znaczący biznes" **– Andy Jassy, CEO AWS-u o generatywnej AI.**

Nowe informacje z branży IT

Allegro pozostaje w polskim DC

Allegro nadal będzie korzystać z centrum danych Talexu. Spółki zawarły aneks do umowy dotyczącej usług kolokacji wraz z usługami towarzyszącymi (outsourcing IT). Szacunkowa wartość kontraktu do końca 2024 r. wynosi 13,1 mln zł netto. Rzeczywista wartość zależy natomiast od faktycznej liczby kolokowanych urządzeń oraz od ilości i zakresu świadczonych usług. Allegro korzysta z centrum danych Talexu od końca 2014 r. Na początku 2019 r. firmy przedłużyły umowę o kolejne 3 lata. Szacunkową wartość 3-letniego kontraktu oceniono wówczas na 11,5 mln zł netto. Warto dodać, że w ostatnich latach wydatki Allegro na usługi centrum danych Talexu rosły, wynosząc w 2022 r. 10 mln zł, tj. ponad dwa razy więcej niż rok wcześniej (4,4 mln zł).

Integratorzy łączą siły

Do grupy Integrity Partners dołączyła Concept Data – warszawska firma, która powstała w 2016 r. Dzięki fuzji Integrity utworzyło nowy pion biznesowy – Identity Security, powiększając tym samym swoje grono ekspertów w tym zakresie. Połączony zespół Concept Data i Integrity Partners liczy ponad 120 osób. Wspólny potencjał ma umożliwić realizację większych i bardziej złożonych projektów. W 2022 r. Integrity Partners miało 84 mln zł przychodów i 6,7 mln zł zysku netto. Warunki finansowe umowy nie zostały ujawnione.

Aukcja 5G rozstrzygnięta

W październiku br. UKE ogłosił wyniki aukcji na cztery rezerwacje po 100 MHz częstotliwości 5G (z pasma 3,6 GHz). Kwota wyjściowa w każdym z bloków wynosiła 450 mln zł (czyli w sumie 1,8 mld zł). W wyniku aukcji stawki sięgnęły poziomu 1,92 mld zł. Tyle wpłacą operatorzy do budżetu państwa. Są to: Polkomtel (450 mln zł), P4 (487,095 mln zł), Orange Polska (487,095 mln zł) i T-Mobile Polska (496,837 mln zł). Cena rezerwacji to dopiero początek niemałych wydatków telekomów. Wyłonione w aukcji podmioty są zobowiązane do inwestycji. W ciągu 4 lat mają uruchomić co najmniej 3,8 tys. stacji bazowych, a 90 proc. powierzchni kraju i 99 proc. gospodarstw domowych znajdzie się w zasięgu internetu o prędkości 95 Mb/s.

Alians Google Cloud i koncernu Solorza

Google Cloud i Grupa Polsat Plus ogłosiły strategiczne partnerstwo. W ramach współpracy lokalne centrum danych amerykańskiego koncernu będzie zasilane energią produkowaną przez farmę wiatrową należącą do Grupy Polsat Plus i ZE PAK. Inwestycja ma kosztować ponad 340 mln zł. Z kolei grupa kontrolowana przez Zygmunta Solorza zmigruje część swojej infrastruktury IT do zasilanych zieloną energią usług chmurowych Google'a. Pracownicy IT spółek grupy (w tym Polkomtela, Netii i Oktawave) zyskają wsparcie szkoleniowe w zakresie rozwiązań chmurowych. Polska grupa będzie też oferować rozwiązania bazujące na Google Cloud, przede wszystkim za pośrednictwem Netii i Oktawave.

121 mln zł za chmurę Microsoftu

Dwie firmy złożyły oferty w „chmurowym" przetargu, w którym Ministerstwo Finansów zamawia doładowania platformy usług hostowanych Microsoft Azure, wraz ze wsparciem technicznym i inżynierskim. Resort zamierza przeznaczyć na sfinansowanie zamówienia 121,2 mln zł brutto. Oferty złożyły dwie firmy: Operator Chmury Krajowej i Integrated Solutions.

Wykonawca musi zapewnić przez okres trwania umowy bezpośredni dostęp do platformy Azure. Termin realizacji przedmiotu zamówienia podstawowego wynosi 36 miesięcy od podpisania kontraktu (opcjonalnie dodatkowe 12 miesięcy). Wymagane jest około 500 roboczogodzin rocznie wsparcia technicznego oraz wparcie inżynierskie producenta na poziomie co najmniej Microsoft Premier Support for Partners Thru Direct. Zamawiający żąda zabezpieczenia należytego wykonania umowy w wysokości 2 proc. ceny ofertowej.

Grupa oszukująca spółki rozbita

Gdańscy funkcjonariusze Centralnego Biura Zwalczania Cyberprzestępczości rozbili zorganizowaną grupę przestępczą, która podszywając się pod inne firmy popełniała oszustwa typu BEC (Business E-mail Compromise). Zatrzymano 11 osób, w tym 6 trafiło do aresztu. W sumie przedstawiono im 72 zarzuty udziału w zorganizowanej grupie przestępczej, oszustw internetowych i prania pieniędzy. Suma strat, jakie poniosły pokrzywdzone firmy, to ponad 13,5 mln zł.

Podejrzani przełamywali zabezpieczenia skrzynek mailowych przedsiębiorstw w kraju i za granicą. Prowadzili fałszywą korespondencję, wysyłając dokumenty bankowe z podstawionymi numerami rachunków. Wyłudzone środki były wypłacane w gotówce albo przelewane na inne rachunki bankowe. Sprawa jest rozwojowa, więc śledczy nie wykluczają kolejnych zatrzymań.

Targi it-sa:
stolica cyberbezpieczeństwa

Norymberga w pierwszej połowie października zamienia się w europejską stolicę cyberbezpieczeństwa. W tym roku targi it-sa zgromadziły nie tylko rekordową liczbę wystawców, ale również gości.

■ *Wojciech Urbanek, Norymberga*

W tym roku do drugiego pod względem wielkości miasta w Bawarii przyjechało 795 wystawców z 30 krajów. Co ważne, prezentowane przez dostawców rozwiązania przyciągnęły bardzo liczną widownię – 19 449 osób, o 30 proc. więcej niż w 2022 r. Pewnego rodzaju ciekawostką jest fakt, że odnotowano 29-procentowy wzrost gości spoza Niemiec, zwłaszcza z krajów europejskich, w tym z Polski.

Organizatorzy it-sa co roku koncentrują się na aktualnych trendach w branży bezpieczeństwa IT, a także dzieleniu się wiedzą i nawiązywaniem kontaktów. Spektrum targowych gości jest dość szerokie i obejmuje administratorów, specjalistów ds. cyberbezpieczeństwa, szefów działów IT, a także kadrę kierowniczą wyższego szczebla. Dodatkową atrakcję tegorocznych targów stanowiła cyfrowa platforma it-sa 365, która zwiększa szanse na nawiązanie kontaktów.

Do najważniejszych wydarzeń w programie towarzyszącym wystawie należała prezentacja inauguracyjna „Hacking the Hackers", którą poprowadził Mark T. Hofmann, analityk ds. przestępczości i wywiadu. Warto też wspomnieć, że w tym roku nagrodę Athene Startup Award UP wręczono firmie Quantum Optics Jena. Na uwagę zasługiwało ponadto stoisko czeskie, na którym swoją ofertę prezentowali dostawcy z kraju naszych południowych sąsiadów. Siłą rzeczy nasuwa się pytanie, czy istnieje szansa, że w przyszłym roku z podobną inicjatywą wystąpi Polska? Przy czym odpowiedź nie jest wcale taka oczywista, zwłaszcza, że w kuluarowych rozmowach można było usłyszeć,

Sophos: cyberbezpieczeństwo jest

„MDR jest nową usługą, i tak jak wszystkie nowe rozwiązania wymaga czasu, aby zyskać szerszą akceptację zarówno wśród klientów, jak i partnerów" – mówi **Sven Janssen, wiceprezes Sophos ds. sprzedaży w regionie EMEA Central.**

CRN Już drugi rok z rzędu mottem Sophos na targach it-sa jest cyberbezpieczeństwo jako usługa. To bardzo szerokie pojęcie, które warto doprecyzować. Na jaki zatem rodzaj usług stawiacie?

Sven Janssen Przede wszystkim od ubiegłego roku konsekwentnie koncentrujemy się na sprzedaży rozwijanych przez nas usług poprzez kanał partnerski. To model, w którym zapewniamy klientom bezpieczeństwo 24 godziny na dobę przez 7 dni w tygodniu. Nie ukrywam, że na początku, kiedy wprowadzaliśmy ten model, nasi partnerzy czuli się nieco zaniepokojeni, że niejako zabieramy im biznes. Jednak w obecnych czasach jest to najlepsza opcja ochrony cyfrowych zasobów w firmach, ponieważ pozwala na bardzo szybkie reakcje. W ten właśnie sposób pozycjonujemy nasze usługi Managed Detection Response.

CRN Jaka jest rola waszych partnerów w tym układzie?

Niektórzy z nich wchodzą w ten biznes, świadcząc usługi. Inni pełnią rolę odsprzedawcy, a Sophos bierze wtedy na siebie zadania związane z obsługą systemu. Współpracujemy też z dużymi partnerami, którzy oferują szeroki wachlarz usług, dla których MDR jest kolejnym składnikiem oferty. Co jednak nie zmienia faktu, że wciąż wielu resellerów sprzedaje firewalle czy zabezpieczenia dla punktów końcowych w modelu tradycyjnym.

CRN W Polsce rosnącą popularnością cieszą się systemy Endpoint Detection and Response. Ich zaletą jest duża efektywność w zakresie wykrywania ataków, a wadą obsługa, do której potrzeba specjalistów. W związku z tym małe i średnie firmy zwykle nie inwestują w te rozwiązania, a jeśli nawet, to okazuje się, że nie radzą sobie z nimi. Jak w tym kontekście pozycjonujecie usługi MDR?

Są przeznaczone zarówno dla dużych, jak i małych przedsiębiorstw. Od czasu, kiedy je wprowadziliśmy, pozyskaliśmy 18 tysię-

że niemieccy klienci z reguły nieufnie podchodzą do dostawców z Europy Środkowo-Wschodniej i flaga czeska lub polska wcale nie musi stanowić wartości dodanej…

Panaceum na brak specjalistów

Osoby słabiej zaznajomione z branżą cyberbezpieczeństwa mogły mieć spore trudności z rozszyfrowaniem skrótów pojawiających się na poszczególnych stoiskach. W tym roku chyba najbardziej rzucał się w oczy akronim XDR, czyli Extended Detection and Response. System ten obejmuje ochronę różnych obszarów – urządzeń, sieci czy danych w środowisku chmurowym, a więc znacznie więcej niż EDR (Endpoint Detection and Response), który zabezpiecza wyłącznie punkty końcowe.

Zdaniem analityków w nieodległej przyszłości sprzedaż tego rozwiązania powinna być dochodowym biznesem. Według MarketsandMarkets wartość globalnego rynku XDR ma osiągnąć w tym roku 1,7 mln dol. Przy czym wszystko, co najlepsze, dopiero przed nami – w 2030 r. ma to być to już 8,8 mln dol. To oznacza, że w latach 2023–2030 skumulowany roczny wskaźnik wzrostu wyniesie 38,4 proc. Rozwiązania XDR były szczególnie mocno promowane na stoiskach Watchguard i Cyberseason. Natomiast Sophos postawił na usługę MDR (Managed Detection and Response), adresowaną zarówno do małych przedsiębiorstw, jak i do korporacji.

– *XDR oferuje większe możliwości w zakresie detekcji i reakcji zagrożeń niż EDR. W związku z tym użytkownicy uzyskują mnóstwo informacji na temat potencjalnych zagrożeń. Niestety, część klientów nie potrafi w pełni wykorzystać potencjału tego rozwiązania, gdyż nie posiadają oni odpowiednich kompetencji. Ten problem rozwiązuje MDR, czyli usługa zarządzanego wykrywania i reagowania na zagrożenia* – mówi Sven Janssen, wiceprezes Sophos ds. sprzedaży w regionie EMEA Central.

W innym obszarze rynku bezpieczeństwa IT działa niemiecka firma baramundi ➤

ciągłym procesem uczenia się

cy klientów, z których większość pochodzi z Europy Zachodniej i Środkowej. We wspomnianych w pytaniu przypadkach rzeczywiście czasami lepiej zamiast EDR wykorzystać antywirusa nowej generacji lub właśnie MDR. Nasz zespół analityków czuwa nad pracą systemu, oferując pomoc w postaci obserwacji sieci i ostrzegania o potencjalnych zagrożeniach.

CRN W segmencie usług cyberbezpieczeństwa najbardziej rozpowszechnionym modelem jest Managed Security Service Provider. Jaka jest zasadnicza różnica pomiędzy MSSP i MDR?

MSSP jest szerszym obszarem do działania dla usługodawców aniżeli MDR. Pozwala bowiem zaoferować szeroką gamę bardzo różnych usług bezpieczeństwa. Część integratorów działa właśnie w tym modelu, co nie przeszkadza im współpracować z nami, ponieważ dajemy im możliwość dodatkowego rozszerzenia pakietu usług o MDR. Co istotne, służymy tutaj wiedzą i doświadczeniami naszych analityków, którzy przez 24 godziny na dobę mają dostęp do informacji nie tylko o tym, co się dzieje w sieci klienta, ale też danych z całego świata.

CRN Jak natomiast oceniacie poziom zainteresowania usługami MDR ze strony partnerów?

MDR jest nową usługą, i tak jak wszystkie nowe rozwiązania wymaga czasu, aby zyskać szerszą akceptację zarówno wśród klientów, jak i partnerów. Szczególnie ważna jest edukacja kanału partnerskiego. Model usługowy oznacza dla sprzedawców duże zmiany związane z restrukturyzacją oferty. Osobny temat to klienci, którzy często preferują zakup rozwiązania i jego obsługę we własnym zakresie. Jednak jak już wcześniej wspominaliśmy, nie zawsze potrafią sobie z tym poradzić. Wówczas dociera do nich, że potrzebują pomocy z zewnątrz.

> **Najgorzej** z atakami ransomware radzi sobie **sektor edukacji.**

CRN Od kilku lat jednym z największych zagrożeń jest ransomware. Niestety, pomimo dostępności wielu narzędzi do ochrony urządzeń, sieci końcowych, systemów backupu, wiele organizacji nie potrafi zastopować napastników. Kto najsłabiej radzi sobie w tej materii?

Z naszych cyklicznych raportów „State of Ransomware" wynika, że jest to sektor edukacyjny. Około 80 proc. placówek doświadczyło w ostatnim roku tego rodzaju ataków. Edukacja tradycyjnie zmaga się z problemem w postaci ograniczonych funduszy na zabezpieczenia, co skrzętnie wykorzystują cyberprzestępcy. Warto dodać, że najniższy poziom ataków odnotowano w branżach IT, nowych technologii i telekomunikacji.

Rozmawiał
Wojciech Urbanek

MATERIAŁ POWSTAŁ WE WSPÓŁPRACY Z FIRMĄ SOPHOS.

software, oferująca systemy UEM (Unified Endpoint Management). To rozwiązania, których popularność rośnie wraz z liczbą obsługiwanych przez firmy urządzeń końcowych. UEM integruje dwa podstawowe obszary IT: jeden wiąże się z zarządzaniem komputerami stacjonarnymi, laptopami, serwerami, zaś drugi smartfonami i tabletami. Oprogramowanie pozwala zarządzać poprawkami i aktualizacjami, egzekwować zasady czy udostępniać urządzenia.

– *W przypadku UEM bardzo ważny jest punkt widzenia administratora, bowiem to on odpowiada za wprowadzanie poprawek na komputerach i za aktualizację systemów. Tak dzieje się od dawna. Nasze nowe podejście polega na poznaniu doświadczeń użytkowników. Chcemy je poprawić poprzez wyjście poza proste monitorowanie i rozwiązywanie zidentyfikowanych problemów* – tłumaczy Marius Brandl, dyrektor sprzedaży w baramundi.

Polacy w Norymberdze

Na targach it-sa pojawiła się nieliczna reprezentacja polskich dostawców. Wśród nich znalazła się między innymi Dagma Bezpieczeństwo IT. Śląski dystrybutor działa na rynku DACH (Austria, Niemcy, Szwajcaria) od 2021 roku, kiedy zarejestrował w Niemczech spółkę DAGMA Gmbh.

– *Dużą popularnością wśród niemieckich klientów cieszy się usługa SOC as Service. W Niemczech, podobnie jak w Polsce, brakuje specjalistów ds. cyberbezpieczeństwa, dlatego coraz więcej firm decyduje się na model usługowy. Naszym atutem jest czytelna oraz elastyczna oferta, dlatego mówimy otwarcie, ile co kosztuje. Nie zmuszamy klientów do przeprowadzania audytów po to, aby otrzymać wstępną wycenę* – mówi Mikołaj Sikorski, Chief Strategy Officer w Dagma Bezpieczeństwo IT.

Stałym bywalcem it-sa jest Rublon, producent rozwiązań do wieloskładnikowego uwierzytelniania użytkowników logujących się do sieci, serwerów, punktów końcowych oraz aplikacji. Większość przychodów firma generuje na rynkach zagranicznych, a zwłaszcza w Stanach Zjednoczonych. Michał Wendrowski, CEO Rublonu, nie ukrywa, że firma ma również apetyt na rynek DACH. Co ważne, firma planuje też zbudować sieć partnerską w Polsce.

Swoją obecność na niemieckim rynku pragnie zaznaczyć również Nacview – polski system Network Access Control (NAC), stworzony przez poznańską firmę Scan IT. To narzędzie do zarządzania dostępem użytkowników i urządzeń do sieci. NAC w przeciwieństwie do modnych systemów EDR czy XDR nie wymaga obsługi ze strony specjalistów, a jedynie odpowiedniej konfiguracji oraz dostosowania do pracy administratora.

– *Współpracujemy już z partnerem z Niemiec i myślę, że nasz produkt ma szanse osiągnąć tutaj sukces. Stawiamy na proste licencjonowanie, dzięki czemu można łatwo oszacować koszt wdrożenia i zakupu systemu. Rozwiązanie Nacview dostosowane jest do obecnych wymagań klientów, oprócz tego nasz system oferuje oryginalne funkcjonalności* – tłumaczy Maciej Salamoński, Business Development Manager w Nacview.

Wiadomo już, że w przyszłorocznej edycji wydarzenia wezmą udział w charakterze wystawców Dagma, Nacview i Rublon. Wiadomo też, że przyszłym roku powierzchnia wystawiennicza powiększy się o kolejną halę. ■

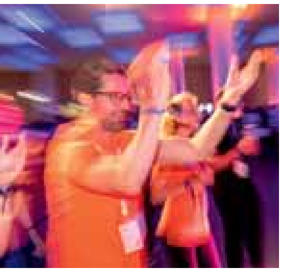
Zdaniem wystawcy

Michał Wendrowski, CEO, Rublon

Targi it-sa to impreza, która na stałe wpisała się w kalendarz wydarzeń IT Security w regionie DACH. Na pewno przyjedziemy tutaj za rok, już zarezerwowaliśmy stoisko w najbardziej prestiżowej hali numer 7. Zdecydowana większość klientów odwiedzających nasze stoisko to Niemcy, zazwyczaj klienci końcowi, rzadziej resellerzy. Znamy już rynek niemiecki, bowiem tutaj działa jedna z naszych spółek Astec, zajmująca się tworzeniem oprogramowania na zamówienie. Jej klientami są między innymi BMW oraz Deutsche Telekom. Zauważamy, że klienci z Niemiec bardzo zwracają uwagę na ochronę danych osobowych swoich pracowników i preferują rozwiązania producentów z Unii Europejskiej. Ponadto, jeśli produkt się sprawdzi, są gotowi za niego zapłacić przyzwoite pieniądze.

Marius Brandl, dyrektor sprzedaży, baramundi software

Nasze stoisko odwiedzają przede wszystkim klienci końcowi, którzy stanowią około 80 proc. naszych gości. Pozostali goście to partnerzy handlowi. Jesteśmy niemieckim producentem, stąd najwięcej naszych partnerów pochodzi właśnie z tego rynku. Jednocześnie cały czas rozwijamy kanał partnerski we Włoszech, Austrii i Szwajcarii, jak też jesteśmy oczywiście obecni w Polsce. Wielu dostawców w czasie tegorocznego it-sa promuje cyberbezpieczeństwo w modelu usługowym. W Niemczech i Polsce jest to stosunkowo nowy rodzaj biznesu. Nasze rozwiązanie nie jest przystosowane do sprzedaży w modelu usługowym. Oczywiście zamierzamy dostosować się do nowych realiów i rozwijamy ten model, ale dopiero rozpoczynamy naszą podróż w tym obszarze. Warto zaznaczyć, że niemieckie firmy nie lubią zbyt gwałtowanych zmian. Dokonują ich wtedy, kiedy muszą.



Rising Stars of Cybersecurity: NIS2 na horyzoncie

Podczas 3. edycji konferencji Rising Stars of Cybersecurity nacisk położono na współpracę DAGMA Bezpieczeństwo IT z integratorami w kontekście dyrektywy NIS2, projektu „Cyberbezpieczny samorząd" oraz usług zarządzanych.

■ ***Karolina Marszałek***

W październikowym spotkaniu wzięli udział integratorzy, których współpraca z dystrybutorem, mimo że rozpoczęta stosunkowo niedawno, rozwija się obiecująco. Nie brakowało firm rozważających działanie w modelu Managed Service Provider. Zainteresowanie budziła prezentacja projektu „Cyberbezpieczny samorząd", który daje szansę na zwiększenie inwestycji w bezpieczeństwo cyfrowe w gminach, powiatach i województwach. Wpisuje się w to m.in. portfolio Stormshielda (nowe wersje rozwiązań i zapowiadany nowy model sprzedaży).

W przypadku ESET-a organizatorzy skoncentrowali się na omówieniu najwyższego i najbardziej zaawansowanego pakietu, czyli ESET PROTECT Elite, zawierającego m.in. funkcje 2FA, Patch Management oraz XDR. Nie zabrakło prezentacji rozwiązania PAM Senhasegura, platformy Holm Security do zarządzania podatnościami na ataki, jak też ofert Acronisa oraz Barracudy (z tym ostatnim producentem DAGMA współpracuje na nowo od sierpnia bieżącego roku).

– *Podczas prezentacji padło wiele przykładów „z życia". Właśnie dzięki takim prelekcjom budujemy świadomość chociażby takich rozwiązań jak Safetica i Acronis, które są bardzo cenione przez naszych klientów* – komentuje Krzysztof Matuszek, specjalista ds. sprzedaży w SQD Alliance.

Wielu uczestników wyraziło ponadto uznanie dla wiedzy prelegentów i nieunikania trudnych pytań.

– *Odpowiadali na nie z marszu. Szczególnie podobała mi się prezentacja dotycząca Stormshielda, która pomoże nam skuteczniej rozmawiać z klientami* – mówi Mariusz Błażejewski, przedstawiciel JawaIT.

NIS2: nie tylko podmioty kluczowe

Podczas wydarzenia podkreślono, że rośnie grupa klientów biznesowych, którzy muszą być przygotowani na wymogi dyrektywy NIS2. Należą do nich nie tylko podmioty kluczowe, czy podmioty istotne. Dyrektywa obejmie też przedsiębiorstwa, które działają w łańcuchach dostaw takich właśnie firm.

– *Wielu przedsiębiorców uświadomiło to sobie niedawno, np. jedno z MPWiK, które jest klientem naszego partnera* – mówi Stanisław Horak, dyrektor handlowy w DAGMA Bezpieczeństwo IT.

Zapewnia przy tym, że rozwiązania oferowane przez dystrybutora stanowią odpowiedź na wymogi dyrektywy.

– *Jesteśmy przygotowani do działania z partnerami w temacie NIS2. Nasze usługi audytowe, wdrożeniowe i szkoleniowe, jak też produkty z naszego portfolio, pokrywają zapotrzebowanie ze strony odbiorców końcowych. Oczywiście partnerzy oczekują od nas praktycznego podejścia, czyli wskazania, które konkretnie rozwiązania sprawdzą się u ich klientów, przygotowujących się na spełnienie nowych wymogów* – mówi Stanisław Horak.

W modelu abonamentowym **partner ma wpływ na cenę.**

MSP: ten model ma potencjał

Specjaliści DAGMY widzą w firmie skokowy wzrost sprzedaży rozwiązań w modelu Managed Service Provider. Również coraz większa liczba partnerów podpisuje dodatkowe aneksy, aby oferować produkty z zakresu cyberbezpieczeństwa w formie usług. Partnerzy, którzy zdecydowali się na ten krok, doceniają zwłaszcza możliwość zarządzania usługami u wszystkich klientów za pomocą jednej konsoli. Podkreślają też elastyczność modelu abonamentowego, co pozwala im zmieniać klientowi z dnia na dzień liczbę chronionych stanowisk. W rezultacie partner rozlicza się miesięcznie za realne wykorzystanie produktów, co może, ale nie musi być elementem jego kontraktu z klientem końcowym.

– *W modelu abonamentowym cenę buduje partner. Im większą liczbą klientów zarządza przez konsolę, tym taniej kupuje usługę, a ostatecznie może więcej zarobić* – mówi Andrzej Wściubiak, Junior Channel Manager w DAGMA Bezpieczeństwo IT.

Usługowy model sprzedaży jest gotowy i funkcjonuje w przypadku rozwiązań dwóch producentów z portfolio katowickiego dystrybutora: ESET-a i Acronisa. Tymczasem dopracowywane są modele MSP kolejnych marek, np. Holm Security.

– *Wdrożenie rozwiązania ESET w ramach usług zarządzanych to jedna z naszych najlepszych decyzji. Samodzielne generowanie licencji daje nam niespotykaną dotąd kontrolę nad procesem sprzedaży i dostarczania usług. Sprawnie reagujemy na potrzeby klienta, oferując mu dostosowane rozwiązania w krótkim czasie* – mówi Maciej Rocławski, partner DAGMA Bezpieczeństwo IT.

Jak dodaje Kamil Giemza, IT Project Manager w Telkonet, model MSP zapewnia atrakcyjne ceny dla klientów i pozwala agregować różne usługi w jednym pakiecie, zwiększając ich wartość. Klienci nie muszą inwestować w infrastrukturę i oprogramowanie. Przy czym klient, któremu integrator zagwarantuje np. pełną ochronę antywirusową w formie usługi, nie będzie się raczej interesować tym, jakiego rozwiązania użyje firma IT. To daje integratorowi swobodę w sięgnięciu po produkt, który się sprawdzi i przyniesie mu oczekiwane profity.

Canalys Forum EMEA: ruszyła gorączka złota

Sztuczna inteligencja nie przeminie jako kolejny „buzzword", ale w znaczący sposób wpłynie na krajobraz kanału sprzedaży IT – przekonywali analitycy Canalysu podczas tegorocznego zjazdu producentów, dystrybutorów i integratorów z regionu EMEA.

■ *Tomasz Gołębiowski, Barcelona*

W ciągu najbliższych pięciu lat wartość sprzedaży rozwiązań i usług związanych z generatywną sztuczną inteligencją osiągnie wartość 158 mld dol. – prognozują analitycy Canalysa. Średni roczny wzrost tego segmentu rynku ma wyraźnie przekraczać 50 proc., co stanowi wyjątkową szansę dla integratorów i niezależnych twórców oprogramowania (ISV). Powinni oni zatem już teraz opracowywać i wdrażać strategie biznesowe w tym zakresie, jak też szukać kompetentnych partnerów – przekonywali organizatorzy tegorocznego Canalys Forum, w którym wzięło udział ponad 1 tysiąc przedstawicieli producentów, dystrybutorów i integratorów z regionu EMEA.

– Generatywna AI nie podzieli losu druku 3D, metawersu, beaconów czy blockchainu, które miały zrewolucjonizować naszą branżę, a okazały się kolejnymi chwytliwymi buzzwordami. Związana ze sztuczną inteligencją „gorączka złota" właśnie ruszyła, a dostawcy IT mają wybór: dostosować się, albo zginąć. Dlatego radzę integratorom, żeby sami zaczęli korzystać z narzędzi AI na swoje potrzeby, takich jak chociażby Bing Chat Enterprise, żeby na bazie własnych doświadczeń prowadzić potem konkretne rozmowy z klientami – zachęcał Steve Brazier, CEO Canalysa.

W tym kontekście Jason Atkins, prezes 360insights – producenta oprogramowania do zarządzania kanałem partnerskim – prognozuje, że w ciągu najbliższych dwóch lat zrewolucjonizowany zostanie sposób konsumpcji firmowych danych. Jego zdaniem „skończy się era analizowania dashboardów, a zamiast tego będziemy po prostu zadawać pytania i uzyskiwać gotowe, konkretne odpowiedzi". Uczestnicy Canalys Forum EMEA mogli też usłyszeć, że potencjał generatywnej AI jest w pewnym zakresie porównywalny do potencjału cloud computingu sprzed dekady, kiedy mało kto zdawał sobie sprawę, z jak rewolucyjną zmianą mieliśmy do czynienia...

> Odpowiedzią na wyzwania jest rozwój **kanału partnerskiego.**

– W przypadku chmury około dziesięciu lat zajęło opracowanie, a potem dopracowanie mechanizmów zarabiania na sprzedaży w modelu subskrypcyjnym. Podobnie w przypadku generatywnej sztucznej inteligencji, rozwój sposobów i form prowadzenia biznesu w tym zakresie nie zakończy się w ciągu najbliższych kilkunastu miesięcy – przewiduje Jay McBain, jeden z głównych analityków Canalysa.

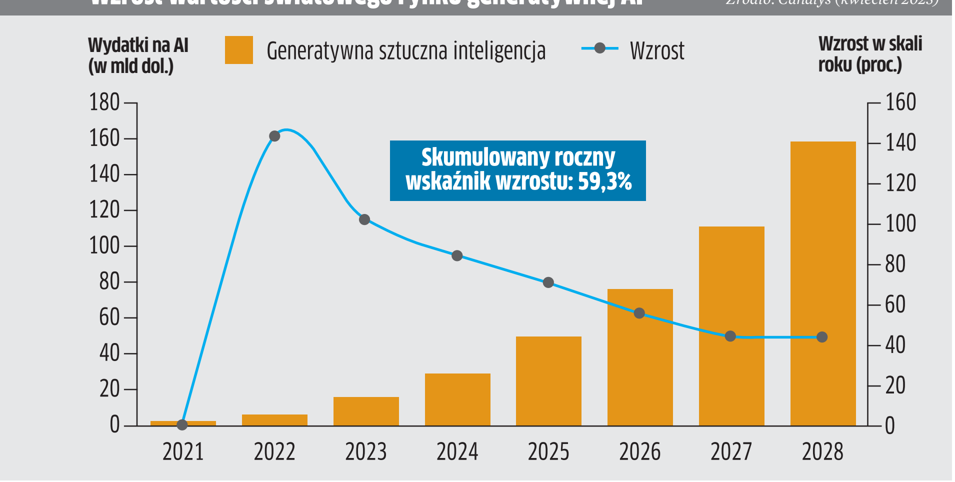
Wtóruje mu Patrick Zammit, szef regionu EMEA w TD Synnex, który podkreślał, że lider światowego rynku dystrybucji potrzebował sporo czasu na przemyślenie oferty i swojej roli w kwestii cloud computingu i tak też ma być w przypadku sztucznej inteligencji.

– Musimy przemyśleć, jak wspierać razem z partnerami użytkowników w procesie implementacji AI w ich organizacjach. To ogromna szansa dla całej branży IT, bo klienci będą w oparciu o sztuczną inteligencję rozwijać swoją infrastrukturę, kontynuując proces cyfryzacji – podsumowuje Patrick Zammit.

Warto dodać, że z danych Canalysa wynika, że aż 59 proc. partnerów w kanale sprzedaży IT z regionu EMEA oczekuje, że zacznie zarabiać na generatywnej AI w ciągu dwóch najbliższych lat. Obecnie 53 proc. takich firm intensyfikuje właśnie wykorzystywanie sztucznej inteligencji na własne potrzeby.

– Teraz jeszcze szybki rozwój sztucznej inteligencji tak bardzo nas nie dotyczy, ale w ciągu

Wzrost wartości światowego rynku generatywnej AI *Źródło: Canalys (kwiecień 2023)*



kolejnych 2–3 lat będziemy ją stosować wewnętrznie na potrzeby powtarzalnych czynności – podsumowuje Hege Store, szefowa skandynawskiego integratora Advania.

Sztuczna inteligencja ma być również siłą napędową na rynku konsumenckim, do czego mają się przyczynić komputery z grupy AI PC. Zgodnie z zapowiedziami, które padały podczas tegorocznego Canalys Forum EMEA, przełom w tym zakresie ma nastąpić w latach 2024–25. Enrique Lores, CEO HP spodziewa się przy tym, że modele z „rodziny" AI PC będą droższe od obecnych ze względu na konkretną wartość dodaną, jaką mają stanowić dla użytkowników biznesowych.

Partnerzy lekiem na zło

Niezależnie od nowych możliwości biznesowych, wielu producentów, dystrybutorów i integratorów uważnie obserwuje perturbacje, z jakimi mamy obecnie do czynienia w świecie polityki i gospodarki. Z mediów płyną do konsumentów, w tym użytkowników biznesowych, negatywne komunikaty dotyczące konfliktów zbrojnych, zawirowań w sektorze finansowym, w tym funduszy inwestycyjnych, jak też wysokiej inflacji i trudnych do przewidzenia skutków deglobalizacji.

– *Odpowiedzią na wiele wyzwań jest rozwój kanału partnerskiego, który radzi sobie w trudnym otoczeniu nadspodziewanie dobrze. Nic dziwnego, że coraz więcej firm przestawia się na ten właśnie model działania* – mówi Steve Brazier.

Z danych Canalysa wynika, że ponad 70 proc. wszystkich światowych wydatków na rozwiązania i usługi IT przechodzi poprzez kanał partnerski, przy czym w wielu sektorach globalnej gospodarki odsetek ten rośnie. Korelują z tym wyniki badań McKinseya, według których globalnie ponad 80 proc. menadżerów na poziomie CEO deklaruje zwiększanie nakładów na rozwój kanałów sprzedaży.

Powyższe działania mają sens między innymi w świetle wyników sprzedażowych kilkudziesięciu największych dystrybutorów i integratorów z regionu EMEA, prezentowanych w ramach stworzonego przez ekspertów Canalysa indeksu EMEA Channel Titans. W I kw. 2023 r. indeks poszybował w górę o 15 proc., podczas gdy indeks Tech Titans, dotyczący kilkunastu największych producentów, skurczył się w tym okresie o 4 proc. (analitycy spodziewają się, że indeks ten zacznie rosnąć wiosną 2024 r.).

Z drugiej strony wielu partnerów z niepokojem obserwuje, że klienci coraz chętniej zamawiają kolejne rozwiązania IT korzystając z usług marketplace'ów. Niemniej, eksperci Canalysa przekonują, że nie ma powodów do paniki.

– *Około 20 procent takich właśnie transakcji jest realizowanych przy udziale integratorów, jak również w asyście dystrybutorów, i ten odsetek będzie rósł. Ponadto za wieloma zamówieniami składanym na marketplace'ach idzie późniejsza obsługa posprzedażna rozwiązań czy aplikacji, świadczona przez kanał partnerski* – podkreśla Alastair Edwards, Chief Analyst w Canalysie.

Podczas tegorocznego Forum EMEA wybrzmiało ponadto, że jednym z kół zamachowych dalszego rozwoju kanału sprzedaży mają być rozwiązania cyberbezpieczeństwa. Analitycy przewidują przy tym, że nawet 16 proc. integratorów w regionie EMEA może w najbliższych latach wypaść z branży, o ile nie zadbają o umiejętności w w tym właśnie obszarze.

Za kolejny katalizator rozwoju branży IT uznano rozwiązania wspierające zrównoważony rozwój w kontekście nowych regulacji, w tym aktualnych i przyszłych zmian w prawie unijnym. Aż 53 proc. firm partnerskich z obszaru EMEA deklaruje, że już w tym roku wygeneruje w ten sposób mniejsze bądź większe przychody. Jednocześnie analitycy Canalysa podają, że ponad 40 proc. klientów nie sprosta wyśrubowanym normom UE dotyczącym zrównoważonego rozwoju, w czym będą mogły im pomóc nowe technologie opracowane i wdrażane przez partnerów w kanale sprzedaży IT.

Czas przełomów w ekosystemie partnerskim

„Jesteśmy świadkami ogromnej zmiany pokoleniowej. Za kilka kwartałów większość kupujących w sektorze IT to będą milenialsi” – mówi **Jay McBain, Chief Analyst w Canalysie.**

CRN Podczas tegorocznego Canalys Forum EMEA najmocniej wybrzmiały dwie kwestie: po pierwsze kanał sprzedaży IT ma się coraz lepiej, a po drugie dużą szansę na jego dalszy rozwój stanowi generatywna sztuczna inteligencja. Skąd ta pewność?

Jay McBain Już teraz świadczą o tym liczby, a konkretnie ponad 15 miliardów dolarów, które rocznie klienci biznesowi wydają na usługi i rozwiązania AI. Wprawdzie to niewielki odsetek całej wartości globalnego rynku IT, ale w ciągu zaledwie pięciu najbliższych lat kwota ta wzrośnie do około 160 miliardów dolarów. Średni wzrost w tym zakresie sięgnie zatem 60 procent, a tego już nie można bagatelizować. Tym bardziej, że dotyczy to rozwoju AI w tak kluczowych obszarach, jak chmura, usługi zarządzane czy cyberbezpieczeństwo. W każdym z tych obszarów generatywna sztuczna inteligencja stanowi biznesową szansę dla firm IT.

CRN Czy jednak, mimo optymistycznych prognoz, nie powtórzy się scenariusz, z jakim mieliśmy do czynienia w przypadku metaverse'u, druku 3D czy beaconów? W Polsce mawiamy o takich przypadkach: z dużej chmury mały deszcz…

W tym przypadku różnica polega na tym, że z możliwości generatywnej sztucznej inteligencji można korzystać na wewnętrzne potrzeby firm IT, w tym integratorów. Dzięki temu można najpierw przebudować swoją własną działalność, pod kątem większej wydajności czy skuteczności. Po czym, na bazie własnych doświadczeń z AI dużo łatwiej i chętniej firmy IT będą zwracały się do klientów z przemyślaną i sprawdzoną ofertą.

CRN Opisany scenariusz wymagać będzie dość długiego czasu…

Tak, wcale nie twierdzę, że to będzie szybki proces. Przeciwnie, spodziewam się scenariusza, jaki miał miejsce w przypadku chmury publicznej, kiedy to Microsoftowi, AWS-owi, Google'owi, a także integratorom zajęło dziesięć lat opracowanie i wdrożenie dobrze działającego modelu sprzedaży. W najbliższych kilku latach dostawcy usług zarządzanych w segmencie generatywnej AI będą mieli niewielkie pole manewru. Natomiast później zaczną pojawiać się usługi i rozwiązania w tym zakresie, za które klienci będą chcieli zapłacić, bo poczują, że w ten sposób kupują rozwiązanie takiego czy innego swojego problemu, bądź realizują ważną potrzebę.

> Dystrybutorzy muszą **wyjść z cienia.**

CRN Kolejnym przełomem, o jakim była mowa podczas Canalys Forum, był „najazd” milenialsów. Co on oznacza?

Jesteśmy świadkami ogromnej zmiany pokoleniowej. Za kilka kwartałów większość kupujących w sektorze IT to będą milenialsi, którzy mają inny niż wcześniejsze generacje sposób myślenia, działania, a w efekcie kupowania. To pokolenie wzmocni chociażby rolę marketplace'ów, w tym AWS-u, który zgodnie z naszymi prognozami miał w 2025 roku trafić do grona dziesięciu największych dystrybutorów IT świata. Tymczasem zdaje się, że nastąpi to szybciej, bo w przyszłym roku.

CRN A co „napływ” milenialsów zmienia w procesie zakupowym?

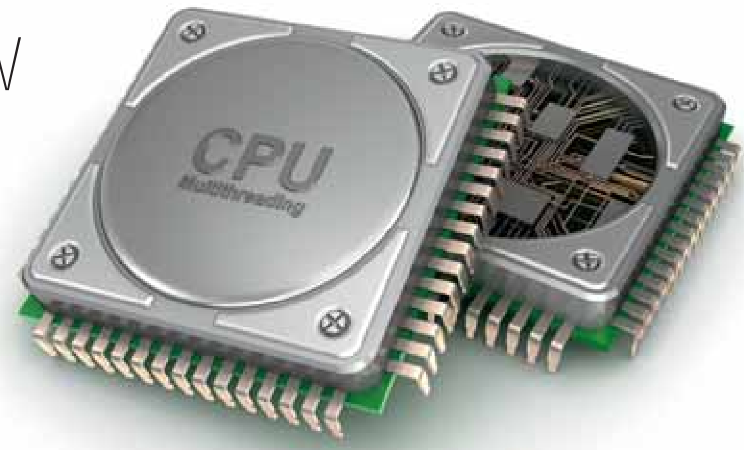
Obecnie proces zakupu składa się z 28 różnych „momentów decyzyjnych”, które prowadzą do jego finalizacji. To czytanie magazynów, słuchanie podcastów, sprawdzanie opinii w mediach społecznościowych, rozmowa ze znajomym, konsultacja ze specjalistą… Z badań McKinseya wynika, że milenialsi w tej „podróży zakupowej” mają średnio aż siedmiu zaufanych partnerów, a raczej doradców. To oznacza znaczny wzrost roli tak zwanych partnerów nietransakcyjnych. Jednym z nich może być chociażby redakcja CRN-a, jako źródło informacji o danym produkcie czy usłudze.

CRN Co to oznacza dla dystrybutorów?

Będą musieli wyjść z cienia, w jakim tkwili przez kilka dekad. Po to, aby pokazać się światu jako specjaliści, wspierający swoich partnerów, a więc pośrednio także użytkowników technologii. Klienci końcowi powinni na swojej ścieżce zakupowej zobaczyć obok integratorów, mediów, youtuberów czy agencji cyfrowych także dystrybutorów. Zwłaszcza, że dystrybutorzy mają odpowiednią wiedzę, możliwości, pieniądze i rozmach. Wśród dystrybutorów są przecież tacy, którzy są większi od tak znanych marek jak Nike, Coca-Cola czy McDonald's, a zupełnie nie są przy tym kojarzeni przez użytkowników technologii. Warto to zmienić, żeby pokazać swoją wartość na całym rynku w dobie rosnącej pozycji hiperskalerów.

Rozmawiał
Tomasz Gołębiowski

Rynek chipów **powraca do zdrowia**



Wiele wskazuje na to, że globalny przemysł półprzewodników osiągnął już swoje dno. Nadszedł czas, żeby się od niego odbić.

■ ***Wojciech Urbanek***

W ostatnich tygodniach szefowie Intela, TSM oraz Samsunga zgodnie przyznali, że najgorszy okres mają już za sobą. I choć Samsung, największy na świecie producent chipów pamięci, odnotował w trzecim kwartale 38-procentowy spadek zysku, to władze koreańskiego koncernu z umiarkowanym optymizmem patrzą w przyszłość. Wiążą to między innymi z rosnącym popytem na nowe modele komputerów osobistych oraz smartfonów wyposażonych w coraz bardziej pojemne pamięci. Kim Jaejune, dyrektor ds. chipów pamięci w Samsungu, uważa, że obecne ożywienie będzie kontynuowane w przyszłym roku.

Wzrost popytu na rynku półprzewodników pokazuje, że globalna gospodarka wykazuje się dość dużą odpornością, radząc sobie z tak poważnymi wyzwaniami jak inflacja, wojna na Ukrainie czy konflikt pomiędzy Izraelem a Hamasem. Chipy są dobrym wskaźnikiem zwiastującym koniunkturę, bowiem używa się ich w wielu produktach, począwszy od komputerów PC i smartfonów poprzez sprzęt w centrach danych, aż po samochody.

Segment półprzewodników będzie rozwijać się **w szybkim tempie.**

Perspektywa poprawy sytuacji uspokoiła rząd Stanów Zjednoczonych, który zgodnie z ustawą CHIPS and Science Act przeznaczył 53 mld dol. na subsydiowanie produkcji półprzewodników. Zresztą sojusznicy USA, w tym kraje europejskie, Japonia i Korea Południowa również wspierają branżę środkami finansowymi lub wsparciem regulacyjnym. Co się opłaci, bo wprawdzie w bieżącym roku globalne przychody z półprzewodników skurczą się o około 12 proc., to analitycy International Business Strategies (IBS) prognozują w 2024 roku 11-procentowy wzrost, a cały omawiany rynek ma być warty 550 mld dol.

Czas na powrót do normalności

W pierwszym roku pandemii znacznie wzrósł popyt na komputery, smartfony, konsole do gier wideo i serwery. Efektem zakupowego szału był niedobór chipów. Cykl zakończył się w 2022 r. wraz z rosnącą inflacją i wojną na Ukrainie. Konsumenci, a także klienci korporacyjni znacznie ograniczyli wydatki na elektronikę. Tym samym zapasy w magazynach producentów sprzętu IT zaczęły rosnąć w niepokojącym tempie.

Producenci półprzewodników, za wyjątkiem tych, którzy wykorzystali boom na sztuczną inteligencję (przede wszystkim Nvidia), ograniczyli produkcję, opóźnili inwestycje, a nawet zwalniali pracowników.

Zysk operacyjny Samsunga na początku bieżącego roku był najgorszy od czternastu lat. Obecnie wraca do „normy", ale kierownictwo koncernu ostrzega, że ożywienie nie będzie tak szybkie, jak spowolnienie, z którym branża borykała się w ubiegłym roku. Niezłe nastroje panują również w Intelu. Pat Gelsinger, dyrektor generalny amerykańskiego producenta, przyznał w rozmowie z The Wall Street Journal, że w tym roku światowy rynek prawdopodobnie wchłonie 270 milionów komputerów, a więc zgodnie z wcześniejszymi oczekiwaniami koncernu. Wprawdzie w trzecim kwartale 2023 r. sprzedaż komputerów skurczyła o 7,6 proc. w ujęciu rocznym, aczkolwiek tempo rocznego spadku zwolniło, co zdaniem IDC wskazuje na poprawę sytuacji, a rynek najgorsze dni ma już za sobą.

Najostrzejszych spadków doświadczyły w ubiegłym roku chipy pamięci, co odczuł między innymi SK Hynix, drugi gracz w tym segmencie po Samsungu. Przedstawiciele tej firmy przyznają, że popyt się odradza, ale sprzedaż układów DRAM osiągnęła rentowność dopiero w III kwartale 2023 r.

Wciąż daleko do boomu

Choć dostawcy półprzewodników wychodzą z kryzysu, mało kto wierzy w powrót do szaleństwa z 2020 r. Sprzedaż smartfonów wciąż jest daleka od oczekiwań producentów, a niepewność gospodarcza w Chinach może ograniczyć popyt na elektronikę. Sporym rozczarowaniem jest rynek samochodów elektrycznych, gdzie analitycy spodziewali się dużo większych wzrostów. Popyt jest tłumiony między innymi przez rosnące ceny energii, wysokie stopy procentowe i niepewność gospodarczą.

Advanced Micro Devices (AMD) przedstawił prognozy na czwarty kwartał bieżącego roku. Producent spodziewa się słabego popytu w segmencie gier wideo, natomiast nadzieję na wzrost wiąże z komputerami PC. Ponadto AMD planuje uzyskać przychody w wysokości 2 mld dol. ze sprzedaży zaawansowanych chipów AI. Co istotne, pomimo różnych turbulencji, segment półprzewodników w najbliższych latach będzie rozwijać się w dość szybkim tempie. Według IBS do 2030 r. wartość globalnego rynku chipów przekroczy bilion dolarów.

Fot. Adobe Stock

CRN XChange EMEA z polskimi akcentami

Zorganizowany przez brytyjską redakcję CRN-a zjazd producentów, dystrybutorów i integratorów z regionu EMEA poświęcony był działaniom M&A, ale także sektorowi cyberbezpieczeństwa.

■ *Wojciech Urbanek, Amsterdam*

Pierwsza konferencja CRN XChange na region EMEA była okazją do zawiązania nowych relacji biznesowych, a także wysłuchania prezentacji, dyskusji panelowych i sesji na temat trendów, możliwości i wyzwań w kanale sprzedaży IT. Swoje portfolio przedstawili: ConnectWise, Kaseya, Huntress, N-able, Scale Computing, Targus oraz ThreatLocker. Wydarzenie zainaugurowała Sarah Shields, dyrektor ds. sojuszy w Computacenter, która opowiadała o zaletach i wadach rozwoju organicznego oraz nieorganicznego. W tej ostatniej materii przedstawicielka brytyjskiego integratora ma bogate doświadczenia, bowiem kilka lat temu brała udział w największej wówczas fuzji w branży IT, czyli połączeniu koncernów Dell i EMC.

– *Wzrost nieorganiczny jest kosztowny. Trzeba wydać pieniądze na zakup firmy, a następnie integrację i zapewnienie zgodności systemów oraz procesów. To przy tym ogromny szok kulturowy dla osób zaangażowanych w fuzję. Należy mieć świadomość, co oznacza rola nabywcy. Pojawiają się specyficzne potrzeby i trzeba do nich podchodzić bardzo ostrożnie, ponieważ w przeciwnym razie można przegrać, stracić przychody, klientów i pracowników* – tłumaczy Sarah Shields.

Firmy rozwijane dzięki przejęciom muszą upewnić się, że „rozumieją DNA", które czyni je wyjątkowymi. Trzeba przy tym znać specyfikę lokalnych rynków, a szczególnie trudnym obszarem jest Europa, gdzie występuje duża różnorodność pomiędzy mieszkańcami poszczególnych państw. Inaczej myślą Włosi, Niemcy czy Skandynawowie i, rzecz jasna, to co działa w jednym kraju, nie sprawdzi się w innym. Czy warto zatem koncentrować się jedynie na wzroście organicznym?

– *Istnieją pewne granice, których nie pokonasz, jeśli będziesz bazować wyłącznie na wzroście organicznym. Nie pozyskasz nowych klientów, nie rozwiniesz nowej linii biznesowej, a z czasem stracisz przewagę konkurencyjną. Dzieje się tak, ponieważ twoi konkurenci stawiają na rozwój nieorganiczny. Tak właśnie jest w tej branży, w której można zjeść lub być zjedzonym* – mówi Sarah Shields.

Z kolei Bart Donne, CEO Computerlandu, w wystąpieniu „Jak być razem silniejszymi" skupił się na omówieniu działań, jakie należy podjąć już po finalizacji połączenia.

– *Jak wiadomo, w wyniku fuzji dwóch firm uzyskujemy efekt synergii. Przychody można zwiększyć poprzez połączenie talentów i technologii czy uzyskanie nowych możliwości w zakresie sprzedaży krzyżowej. Jednak, aby osiągnąć te cele, trzeba tworzyć odpowiednią atmosferę, ponieważ pracownicy połączonych podmiotów często ze sobą konkurują. Ważny jest tu obustronny szacunek* – przekonuje Bart Donne.

Zdaniem integratora

■ **Grzegorz Świrkowski, CEO, Net Complex**

W dobie cyfrowej rzeczywistości znaczenie granic państwowych i kontynentalnych staje się coraz mniej wyraźne, co zostało mocno zaakcentowane podczas konferencji CRN XChange EMEA. To wydarzenie, skupiające się przede wszystkim na kwestiach cyberbezpieczeństwa w globalnym wymiarze, uświadamia nam, że zagrożenia w cyberprzestrzeni są wszechobecne i dotyczą każdego, niezależnie od miejsca, w którym się znajduje. Miałem przyjemność uczestniczyć w tej innowacyjnej konferencji wspólnie z CRN Polska. Jestem pod wrażeniem produktów, które zostały tam zaprezentowane. Idealnie odpowiadają one na potrzeby naszych klientów, którzy szukają skutecznych rozwiązań do ciągłego audytu i monitorowania kondycji ich infrastruktury IT. W najbliższym czasie planujemy przedstawić produkty, które poznaliśmy na konferencji i które wpisują się w dyrektywę NIS2.

■ **Bartłomiej Domański, właściciel, Komplus**

Wyjechaliśmy z konferencji CRN XChange EMEA z trzema zapamiętanymi słowami: Cybersecurity, Sustainability, Diversity. Cyberbezpieczeństwo było tematem większości wykładów i spotkań. Konferencja pokazała nam jak powszechne jest w Zachodniej Europie zastosowanie zaawansowanych rozwiązań cyberbezpieczeństwa. Często poruszanym zagadnieniem był też zrównoważony rozwój biznesu. Na konferencji zobaczyliśmy interesujące produkty monitorujące zużycie prądu na stanowisku lub informujące o pozostawieniu na noc włączonego komputera. Ostatnim tematem, na który zwróciliśmy uwagę, było korzystanie z potencjału ludzi z dysleksją, spektrum autyzmu czy ADHD. Reasumując, konferencja była dla nas bardzo ciekawym wydarzeniem, na którym zdobyliśmy sporo świeżej wiedzy oraz relacji z partnerami z zagranicy i Polski.

Jeśli pomiędzy pracownikami będzie dochodzić do licznych niesnasek i niezdrowej rywalizacji, odbije się to w negatywny sposób nie tylko na przychodach, ale również wizerunku organizacji. Tym bardziej, że konkurenci czyhają na takie okazje.

– Niestety, często się zdarza, że po połączeniu dwóch firm odchodzą z nich najlepsi ludzie. Dlatego menedżerowie muszą być szczerzy i na poważnie zaangażować się w budowanie dobrych relacji z pracownikami. Tym bardziej, że to oni pełnią rolę ambasadorów przedsiębiorstwa - zauważa Bart Donne.

Nie taka znów tania chmura

Wiele wskazuje na to, że fascynacja usługami chmurowymi powoli przemija. Wprawdzie chmura publiczna nadal spełnia ważną rolę w cyfrowej transformacji, aczkolwiek przedsiębiorcy dostrzegają jej mankamenty. Michael Stephens, wiceprezydent ds. partnerstwa w Aptum Technologies, zwraca uwagę na fakt, iż CIO, którzy decydowali się na migrację do środowiska chmurowego przede wszystkim ze względu na koszty, wpadli w pułapkę. Nagle okazało się, że sytuacja wymyka się im spod kontroli, ponieważ przestali sobie radzić z kontrolą i zarządzaniem kosztami usług chmurowych.

W badaniu przeprowadzonym przez Aptum Technologies wśród 100 specjalistów IT, aż 73 proc. respondentów stwierdziło, że inwestycje w chmurę publiczną były wyższe aniżeli pierwotnie przewidywali, a według 52 proc. nieefektywność chmury sprawiła, że zmarnowali znaczną część wydatków na IT. Co ważne, przeciętny klient korzysta z usług siedmiu różnych dostawców usług chmurowych, a tymczasem...

– W ciągu ostatnich kilku lat niejednokrotnie spotykałem się z sytuacją, że firmy wysyłały pracowników na specjalistyczne szkolenia dotyczące chmury, po czym pracownicy już z nich nie wracali do swoich pracodawców, bo przy okazji ktoś zaoferował im lepiej płatne zajęcie – mówi Michael Stephens.

Aptum Technologies działa jako Managed Service Provider, oferując konsulting, a także rozwiązania do optymalizacji usług chmurowych. Kluczową kwestią jest w tym przypadku dokładna analiza obciążeń. Na tej podstawie można wyciągać wnioski, a następnie podjąć działania zmierzające do racjonalizacji kosztów. Jednym z najczęściej popełnianych przez klientów usług chmurowych jest niewykorzystanie zasobów udostępnianych w ramach umowy przez usługodawcę.

Październikowa konferencja CRN XChange była pierwszą w regionie EMEA. Wcześniej podobne spotkania były organizowane z myślą o producentach, dystrybutorach oraz integratorach ze Stanów Zjednoczonych. Każda kolejna edycja stanowi mieszankę szeregu informacji na temat technologii, budowania relacji w kanale sprzedaży, a także sposobów rozwoju biznesu na dynamicznie zmieniających się rynku IT. Na uwagę zasługuje fakt, że w edycji EMEA wzięło udział siedem firm z Polski: Cloudica, Engave, Fast IT, Infonet Projekt, Komplus, Net Complex oraz Senetic. Było to najliczniejsza, obok brytyjskich, grupa integratorów z jednego rynku. Redakcja CRN Polska dziękuje wymienionym firmom za przyjęcie zaproszenia i ma nadzieję na spotkanie podczas CRN XChange EMEA 2024.

Adam Kotecki, CEO, Cloudica

Agenda CRN XChange EMEA była wypełniona mnóstwem spotkań, prezentacji i warsztatów. Główną oś konferencji stanowił obszar szeroko pojętego cyberbezpieczeństwa. Mnie zainteresowały szczególnie takie rozwiązania, jak: Threatlocker, Kaseya i Huntress. Fascynującą prezentację miała również firma ScaleComputing, przedstawiając koncepcję Edge Computing opartą na idei samonaprawialności i samokonfiguracji platformy przy zachowaniu wysokiego poziomu bezpieczeństwa i wydajności. „Jestem CEO, jestem odpowiedzialny za kulturę w firmie", a więc hasło z jednego z wykładów o ekspansji zagranicznej i jej uwarunkowaniach, dobrze zgrało się z moją wizją firmy. Rolą kadry zarządzającej, a CEO w szczególności, jest stworzenie optymalnego, bezpiecznego, otwartego, ambitnego środowiska pracy i rozwoju.

Sławomir Zieliński, CEO, Fast IT

Udział w konferencji CRN XChange EMEA w Amsterdamie był dla mnie doskonałą okazją do pogłębienia wiedzy o obecnych trendach, które kształtują naszą branżę i wpływają na warunki prowadzenia biznesu przez integratorów IT i MSP. Jedną z największych wartości tego spotkania było zebranie ekspertów, dostawców, przedsiębiorców i pasjonatów technologii z wielu krajów. Ta impreza to nie tylko platforma do wymiany wiedzy, ale także inspirujące doświadczenie, które pozwala zrozumieć, w jaki sposób innowacje będą kształtować naszą przyszłość. Warto podkreślić, że CRN XChange EMEA to doskonała okazja do nawiązania cennych kontaktów zawodowych. To także idealne miejsce, aby poznać ludzi, którzy dzielą pasję do nowych technologii i chcą wspólnie tworzyć przyszłość.

Zarządzanie danymi,

czyli trudna sztuka wyboru rzeczy ważnych

CRN Stowarzyszenie DAMA Poland działa w ramach organizacji DAMA International – The Global Data Management Community. Jesteście jednym z jej 83 autoryzowanych przedstawicielstw funkcjonujących w 47 krajach. Jakie cele stawia sobie wasza organizacja?

Tomasz Nitsch Działamy na rzecz promowania wiedzy i profesjonalnych standardów w obszarach związanych z gromadzeniem, przetwarzaniem, wykorzystywaniem i ochroną danych. Umożliwiamy też wymianę doświadczeń i dzielenie się dobrymi praktykami w tym zakresie. Jesteśmy organizacją niezależną od producentów. Proponujemy zatem rozwiązania, które nie są powiązane z interesami dostawców konkretnych narzędzi informatycznych. DAMA International ma kilkudziesięcioletnią historię, choć okres jej wzmożonej ekspansji światowej przypada na ostatnie 10 lat. Polski oddział powstał 5 lat temu, a grupa inicjatywna zawiązała się podczas konferencji CDO Forum.

CRN Czy do organizacji należą głównie ludzie pracujący na takich stanowiskach jak Chief Data Officer?

Generalnie są to zazwyczaj osoby pełniące funkcje menedżerskie związane z danymi, w tym CDO. Ale jesteśmy otwarci na wszystkich zainteresowanych zarządzaniem danymi, czyli również dostawców usług czy studentów. Warto wspomnieć, że chociaż w polskich firmach coraz częściej powoływane są specjalne jednostki organizacyjne oraz osoby w roli CDO, to ciągle zarządzaniem danymi zajmują się zwykle eksperci rozsiani po różnych departamentach i pracujący na różnych stanowiskach.

Nie ma też jednego, uniwersalnego modelu organizacyjnego. Z jednej strony data management bywa usytuowany przy dziale finansowym. Argumentem za wyborem tej opcji jest założenie, że tam właśnie przetwarza się najwięcej kluczowych danych firmowych, którym można zapewnić ścisłą kontrolę dzięki podejściu opartemu na liczbach. Z drugiej strony zarządzanie danymi lokuje się w pionie IT, bo tam odbywa się przetwarzanie danych i można je zorganizować w taki sposób, by przynosiło to firmie jak najwięcej korzyści. Reszta stosowanych modeli zarządzania danymi mieści się w zasadzie między tymi dwoma brzegowymi scenariuszami. Częstym rozwiązaniem jest budowanie zespołów interdyscyplinarnych, w skład których wchodzą ludzie z departamentów biznesowych, finansowych i IT. Chief Data Officer ma być osobą, która będzie łączyła wszystkie te światy poprzez nałożenie na nie perspektywy zarządzania danymi.

> Kluczową rolę odgrywa **etykietowanie danych.**

CRN A jak jest umocowany Chief Data Officer w Banku Millennium i jaki model zarządzania danymi realizujecie?

W naszym banku nastąpiło przeniesienie zarządzania danymi z pionu finansowego do pionu IT. Powołano przy tym zespół do zarządzania procesami danych. I to właśnie za pracę tego zespołu jestem odpowiedzialny jako Chief Data Officer.

CRN Jakie racje stoją za przyjęciem obecnego rozwiązania?

„Rolą CDO, i to bardzo ważną, jest zapewnienie organizacji tak zwanego Data Culture, czyli zadbanie o zrozumienie i przestrzeganie określonych reguł pracy z danymi na poziomie każdego pracownika firmy, a nie tylko zarządu, finansów czy działu IT" – mówi **Tomasz Nitsch, Chief Data Officer w Banku Millennium i prezes zarządu DAMA Poland Chapter, organizacji zrzeszającej profesjonalistów zajmujących się danymi.**

Powodów, jak zwykle w takich sytuacjach, można wymienić co najmniej kilka. Szczególnie istotne znaczenie ma możliwość dobrej operacjonalizacji prowadzonych działań. Jedną sprawą jest bowiem dobre ustawienie procedur i wyznaczenie osób ze sfery biznesowej – data ownerów i data stewardów, umiejących opisać dane i czujących się za nie naprawdę odpowiedzialnymi. Inną kwestią jest natomiast uruchomienie i prowadzenie aplikacji, które są pomocne w tych właśnie procesach. Ważne jest też przy tym zapewnienie obsługi błędów związanych z danymi. A dość często zgłoszenia z tego zakresu i tak są przekazywane do realizacji specjalistom z pionu IT.

CRN W niektórych firmach istnieje jednak obawa przed oddawaniem zarządzania informacją w ręce działów IT, które są traktowane głównie w kategoriach wsparcia technicznego.

Obawy wynikają przede wszystkim z założenia, że ludzie od IT nie rozumieją biznesu. Jak zatem można przekazać im odpowiedzialność za kluczowe dla prowadzonej działalności procesy? Zakłada się, że będą podejmować działania optymalne z technicznego, ale nie biznesowego punktu widzenia. W kontekście jakości danych będą zaś dążyć do ich poprawności technicznej, a nie wartości biznesowej. Myślę jednak, że tego typu postrzeganie działów IT jest już coraz rzadsze, a eksperci z IT pokazali niejednokrotnie swoją kluczową rolę we wspieraniu biznesu.

CRN Z drugiej strony, w wielu firmach wciąż jeszcze informacja jest utożsamiana z informatyką...

W firmach coraz częściej daje o sobie znać poważny problem, związany z narastającą ilością danych. Pochodzą one już nie tylko z wewnętrznych baz danych czy aplikacji, ale są generowane w olbrzymich ilościach także przez strony internetowe, IoT, media społecznościowe, serwisy sieciowe itp. Konieczna jest odpowiedź na pytanie, jak sobie poradzić z przetwarzaniem takich ilości danych i jak efekty tego przetwarzania zamienić w dobre decyzje biznesowe? Ze strony działu IT istnieje – wynikająca z posiadanych możliwości – pokusa zajęcia się tym zadaniem. Na przykład skoro monitorując aktywność internetową mamy techniczne możliwości rejestrowania wszystkich kliknięć i akcji, to dlaczego nie mielibyśmy poddać uzyskanych danych obróbce. Pytanie tylko: po co? Odpowiedzi muszą udzielić przede wszystkim przedstawiciele środowiska biznesowego. Działania w obszarze zarządzania danymi muszą odpowiadać oczekiwaniom strategii biznesowej przedsiębiorstwa, a nie wynikać tylko z technicznych możliwości przetwarzania danych. Bez względu na to, gdzie rola CDO jest umiejscowiona.

CRN To odwróćmy nieco perspektywę: w jakim zakresie to, co robią ludzie odpowiedzialni za zarządzanie danymi, wpływa na funkcjonowanie firmowych działów IT?

Rolą i zadaniem CDO jest przede wszystkim określenie zasad data governance, czyli polityki zarządzania danymi. Chociaż czasami w jego gestii jest też wiele innych rzeczy, łącznie z analityką czy hurtownią danych, to zawsze w zakres jego odpowiedzialności wchodzi data governance sensu stricto. To oznacza konieczność określenia takiego ➤

Fot. archiwum

zakresu danych, o które chcemy, jako organizacja, zadbać w sposób szczególny, bo widzimy, że działając przy ich użyciu i w oparciu o nie osiągniemy rzeczywiste korzyści. Rolą CDO, i to bardzo ważną, jest też zapewnienie organizacji tak zwanego Data Culture, czyli zadbanie o zrozumienie i przestrzeganie określonych reguł pracy z danymi na poziomie każdego pracownika firmy, a nie tylko zarządu, finansów czy działu IT. Dział IT musi natomiast zapewnić odpowiednie możliwości techniczne przetwarzania wskazanych danych i dostępu do nich.

CRN Od czego w praktyce zaczyna się zarządzanie danymi?
Zarządzanie danymi powinniśmy rozpocząć od kroku, który niejednokrotnie jest pomijany, czyli zbudowania strategii danych – określenia, które dane są istotne w kontekście celów organizacji. Promowane przez DAMA podejście zakłada wydzielenie poszczególnych domen czy obszarów danych i przypisanie im właścicielstwa. Podziału można dokonać według różnych kryteriów, na przykład pod względem produktów. Następnie w ramach tak wydzielonych grup należy zastanowić się, co jest w danym obszarze najważniejsze. Powinni zostać wyznaczeni właściciele danych – data owners – oraz opiekunowie danych – data stewards – dla każdej z tych linii biznesowych. Konsekwentnie, w porozumieniu z nimi należy dokonać opisu poszczególnych produktów kilkoma podstawowymi, najbardziej istotnymi parametrami. W innym podziale jedna osoba może odpowiadać za bazę klientów, druga za bazę produktową, zaś trzecia za bazę HR itd. W każdym przypadku niezmiernie istotne jest ustalenie podstawowego zestawu danych kluczowych w danej grupie, mających pierwszoplanowe znaczenie z pespektywy prowadzonego biznesu.

CRN Na jakiej podstawie dokonuje się wyboru tych danych?
Zazwyczaj na bazie wiedzy eksperckiej data ownerów i data stewardów z uwzględnieniem strategii biznesowej firmy. Na właścicieli danych wyznaczane są przeważnie osoby kierujące departamentami odpowiedzialnymi za dany obszar działalności. Natomiast opiekunami danych stają się pracownicy posługujący się daną grupą danych na poziomie operacyjnym. Ważne, by każdy zestaw danych korespondował ze strategicznymi wytycznymi firmy. Jeśli, załóżmy, bank wdraża popularną obecnie w sektorze finansowym hiperpersonalizację, czyli dokładne zrozumienie oczekiwań klienta, to musi mieć możliwość zweryfikowania poprzez bazę danych, na przykład bazę wykonywanych operacji bankowych, potrzeb i możliwości finansowych poszczególnych klientów. Chodzi o to, żeby wiedzieć, jaką pożyczkę można zaproponować klientowi bez zbędnego ryzyka. Jeśli z kolei strategia zakłada ogólnie lepsze odpowiadanie na potrzeby rynku, to musimy wiedzieć, jakie dane do realizacji tego celu będą przede wszystkim potrzebne i skąd je pozyskać. Może się wtedy okazać, że powinniśmy pobierać więcej danych ze źródeł zewnętrznych, na przykład z portali społecznościowych, żeby wiedzieć czego klienci potrzebują. Tutaj coraz bardziej przydatne okazują się być rozwiązania bazujące na sztucznej inteligencji, umożliwiające chociażby szybką analizę tzw. sentymentu, czyli jaki wydźwięk emocjonalny ma dana wypowiedź.

> **Przenieśliśmy zarządzanie danymi do pionu IT.**

CRN Czy coraz powszechniejsze stosowanie narzędzi bazujących na sztucznej inteligencji przynosi jakieś nowe, specjalne wyzwania dla osób zajmujących się zarządzaniem danymi w firmach?
Przede wszystkim musimy zadbać o dobre etykietowanie danych, ich labelizację, jak mówimy z angielska. To jest podstawowe zadanie w zarządzaniu danymi, szczególnie wtedy, gdy korzystamy ze sztucznej inteligencji. Do każdej danej – a takimi danymi mogą być również dane nieustrukturyzowane, takie jak obrazy czy pliki audio – przypisujemy określone cechy. Taką cechą może być wskazanie stopnia istotności danego atrybutu, jak również określenie jego rodzaju, na przykład czy zawiera dane osobowe, jaki jest aktualnie poziom jej aktualności itp. Im lepiej zrobione jest etykietowanie, tym dokładniejsze rezultaty daje bazujący na niej model. Oczywiście im więcej przypisanych cech, tym lepsze rezultaty można osiągnąć. Nie można jednak skupić się tylko na samym etykietowaniu danych, bo to można by robić w nieskończoność. Zawsze trzeba wyważyć, ile i jakie cechy potrzebujemy określić, żeby procesy mogły sprawnie działać.

CRN Mówi się, że przy korzystaniu ze sztucznej inteligencji ważne jest zapewnienie jak najlepszej jakości danych, które stanowią chociażby podstawę trenowania modeli uczenia maszynowego. Jak w bieżącej praktyce działalności biznesowej zapewnić realizację tego postulatu?
To prawda, zasada GIGO – śmieci na wejściu, śmieci na wyjściu – nie straciła nic ze swej istotności. Konieczne jest jednak wyraźne rozróżnienie. Czym innym jest etykietowanie danych, a czym innym data quality, czyli jakość danych. Etykietowanie to opis danych – jest ono wbrew pozorom ważniejsze dla procesów bazujących na sztucznej inteligencji niż jakość danych. Bo musimy w pierwszym rzędzie wiedzieć, jak istotnych i na ile pewnych dla określonej sytuacji danych używamy.

CRN Czyli mówimy tu bardziej o metadanych, a więc danych opisujących dane…
Tak, metadane są bardzo ważne. Załóżmy, że chcemy zrobić analizę, która nam wskaże, komu warto wysłać specjalną ofertę. Przygotowaliśmy na tę potrzebę bazę składającą się w połowie z danych pozyskanych od zewnętrznego dostawcy zawierającą szerokie spektrum informacji o potencjalnym partnerze, a druga połowa pochodzi z naszej bazy klientów, więc ogranicza się do historii wzajemnej współpracy.
Mając tak pokategoryzowane zbiory jesteśmy w stanie przeprowadzić bardziej wiarygodną analizę. Korzystając

z odpowiednich algorytmów można na przykład ocenić, czy w danej kwerendzie bardziej powinniśmy polegać na pełnych danych, ale z niepewnego źródła, czy też odwrotnie – na niepełnych danych, ale z pewnego źródła. Ostateczna decyzja odnośnie do zasad kategoryzacji danych zależy w dużej mierze od strategii firmy – czy bardziej zależy jej na wchodzeniu na nowe rynki, czy na eksplorowaniu obecnych klientów. Strategia zaś przekłada się na operacyjne zarządzanie danymi – określenie, jakich danych potrzebujemy, albo jakich możemy użyć, żeby móc podejmować właściwe decyzje biznesowe.

CRN Gdzie tu jest miejsce na zarządzanie jakością danych?

Jakość danych jest w dużej mierze pochodną klasyfikowania danych. Ustalamy, że tych 10 danych, na przykład w odniesieniu do produktu, ma dla nas kluczowe znaczenie, kolejnych 10 już mniejsze, a tych 10 ostatnich jest najmniej ważnych. Przykładowo: w bazie dowodów osobistych znacznie ważniejszą informacją jest termin ważności niż organ wydający dokument. Przyjmujemy, że przynajmniej każdy najważniejszy atrybut musi mieć miernik jakości danych, który pomoże nam określić, czy posiadane przez nas dane są rzeczywiście dobre. Dla najmniej ważnych atrybutów określa się mierniki jakości w zasadzie tylko w sytuacji wyraźnie umotywowanej potrzeby. Zawsze trzeba brać pod uwagę relację kosztów i nakładów do oczekiwanych oraz faktycznie otrzymywanych rezultatów.

CRN Jak na poziomie operacyjnym odbywa się sprawdzanie jakości danych?

To bardzo proste. Zazwyczaj wprowadzane są różnorakie walidacje przy wprowadzaniu danych do systemów. A dodatkowo przygotowujemy odpowiednie reguły sprawdzające, które są implementowane do oprogramowania działającego w sposób automatyczny. Konkretny kształt tych reguł może być różny w zależności od stosowanego software'u, na przykład można użyć zapytań SQL-owych. Załóżmy, że sprawdzamy dane w bazie klientów detalicznych. Zestawiamy zarejestrowany PESEL i płeć klienta. Wiadomo, że w numerze PESEL jest zaprogramowana płeć – jeżeli obie zapisane w bazie wartości się zgadzają, to znaczy, że dana jest odpowiedniej jakości. Baza „odpytywana" jest na okoliczność ustalonego kryterium cyklicznie, zazwyczaj raz na miesiąc. Częstotliwość sprawdzeń jest zazwyczaj wynikiem kompromisu między potrzebami biznesowymi a nadmiernym obciążeniem infrastruktury teleinformatycznej.

CRN A co się dzieje, gdy zostaną wykryte nieprawidłowości w danych?

Informacja na ten temat jest przekazywana do Rady ds. Data Governance. Rolą tego ciała jest ustalenie przyczyn zauważonych odstępstw od normy i zainicjowanie działań naprawczych. W praktyce zazwyczaj sprawa trafia do właściciela danych z prośbą o wyjaśnienie powodów zaistniałych błędów bądź uruchomienie procedur przywrócenia ustalonego poziomu jakości danych. W konkretnie określonych przypadkach mogą też być od razu wskazywani opiekunowie danych jako osoby właściwe do doprowadzenia do usunięcia nieprawidłowości. W zależności od wagi, od znaczenia danego rodzaju danych dla działalności firmy akcje naprawcze mogą być podejmowane w trybie natychmiastowym np. w przypadku błędów uniemożliwiających obsługę klienta lub dopiero po przekroczeniu ustalonego poziomu błędu. Przykładem takiej sytuacji może być posiadanie w bazie klientów o nieważnych dowodach osobistych czy braku adresu e-mail. Przy pojedynczych przypadkach jest to akceptowalne, ale w dużej skali takie marnej jakości dane mogą wpłynąć na rezultaty biznesowe. Dlatego należy podjąć działania poprawiające biznesową jakość danych chociażby poprzez akcję promującą zgody marketingowe i przekazywanie adresów e-mail.

> Warto **zadbać o poprawę** biznesowej jakości danych.

CRN Często mówi się dzisiaj, że najlepsze perspektywy biznesowe otwierają się przed firmami, które są „sterowane" danymi – data driven companies. Co to w praktyce oznacza?

To bardzo modne dzisiaj hasło. Na poziomie buzzwordu jest rzeczywiście bardzo atrakcyjne. Zastanówmy się jednak, jakie powinny być faktycznie konsekwencje wprowadzenia go w życie. Co tak naprawdę znaczy data driven company? Gdyby trzymać się ściśle tego określenia, to by oznaczało, że jeśli z analizy danych przy określonych kryteriach wyjdzie, że nasze sklepy nie powinny być otwarte w porze obiadowej, bo wtedy są nierentowne, to wbrew opinii wszelkich menedżerów i pracowników taka zmiana powinna zostać wprowadzona. To jest prawdziwe data driven company, kiedy decyzje biznesowe podejmowane są z automatu na podstawie posiadanych danych. Stąd ta metoda jest stosowana raczej do detalicznych decyzji jak np. uzupełnienie stanu pojedynczego produktu w sklepie.

CRN Czy zatem wszyscy, którzy używają tego hasła, są dzisiaj rzeczywiście gotowi na pełne, konsekwentne wprowadzenie go w życie?

Myślę, że w większości przypadków mamy na razie jeszcze do czynienia z data informed business, czyli że na podstawie danych generujemy możliwie jak najlepsze modele, najlepsze podpowiedzi do podejmowania decyzji. Żeby robić prawdziwe data driven company, trzeba mieć przede wszystkim zaufanie do danych, wiedzieć, że są pewne i naprawdę istotne dla naszego biznesu. Taką pewność można zbudować przez umiejętne zarządzanie danymi. A w procesie tym kluczową rolę odgrywa wspominana już wcześniej klasyfikacja danych, która pozwala nam zachować kontrolę nad naprawdę wartościowymi z naszego punktu widzenia danymi nie tracąc czasu i zasobów na zajmowanie się danymi mniej istotnymi lub w ogóle nieistotnymi.

Rozmawiał
Andrzej Gontarz

Cyberbezpieczeństwo: koniec obietnic, czas na dowody

Na przestrzeni kilku ostatnich lat w segmencie produktów do ochrony urządzeń końcowych zaszły istotne zmiany. Nowoczesne narzędzia otwierają nowe możliwości w zakresie zabezpieczania sprzętu, ale niosą też ze sobą pewne wyzwania.

■ *Wojciech Urbanek*

Fot. Adobe Stock

W większości przypadków firmy, które chcą zabezpieczyć swoją infrastrukturę informatyczną, polegają na obietnicach producentów. Dyrektor działu IT, podpisując umowę z dostawcą zabezpieczeń, kupuje obietnicę, że system bezpieczeństwa IT powstrzyma atak hakerów i zapobiegnie naruszeniom danych. Ten model jakoś działa, a część dostawców wywiązuje się ze swoich obietnic, zapobiegając najczęstszym rodzajom ataków. Jednak najbardziej dojrzali specjaliści ds. cyberbezpieczeństwa zrozumieli, że wbrew temu, co opowiadają marketerzy, powstrzymanie wszystkich naruszeń jest niemożliwe.

Nie bez przyczyny coraz głośniej mówi się o konieczności przejścia od obietnic do dowodów. Co istotne, bazowanie na dowodach nie oznacza wcale rezygnacji z zapobiegania atakom. Nowe podejście uwidacznia się między innymi w sektorze rozwiązań do ochrony urządzeń końcowych. Koniec ery tradycyjnego oprogramowania antywirusowego zapowiedział w 2014 r. Brian Dye. Ówczesny wiceprezydent Symanteca pozwolił sobie na odrobinę szczerości, wyznając na łamach New York Timesa, że antywirusy zatrzymują jedynie około 45 proc. cyberataków.

Nic dziwnego, iż w końcu sami użytkownicy zaczęli bliżej przyglądać się antywirusom. Wprawdzie nie okazało się, że król jest nagi, ale z pewnością bardzo skromnie przyodziany. W międzyczasie na rynku zadebiutowały nowe produkty, takie jak Next Generation Antivirus (NGAV), Endpoint Detection and Response (EDR), Endpoint Protection Platforms (EPP), a od niedawna XDR (Extended Detection and Response). Pierwszy z wymienionych produktów jest niejako naturalnym następcą antywirusa. Z tym, że NGAV w przeciwieństwie do swojego protoplasty nie bazuje wyłącznie na sygnaturach wirusów i jest bardziej zorientowany na prewencję aniżeli reakcję. Antywirus nowej generacji wykorzystuje do identyfikacji zagrożeń kombinację sztucznej inteligencji, wykrywania behawioralnego i algorytmów uczenia maszynowego.

> Część klientów jest **zagubiona i niezdecydowana.**

NGAV ma jeszcze jedną dużą zaletę, czyli rozpoznawanie nieznanego złośliwego oprogramowania i wysublimowanych ataków poprzez analizę całego kontekstu, a nie tylko odosobnionych incydentów. Bogata informacja kontekstowa pozwala NGAV zrozumieć przyczynę ataku, a tym samym zapobiec przyszłym incydentom. Zdaniem specjalistów ds. cyberbezpieczeństwa antywirus nowej generacji jest niezbędnym minimum dla firm poważnie podchodzących do ochrony urządzeń końcowych.

EDR na fali wznoszącej

Wszystko wskazuje na to, że w nadchodzących latach wzrastać będzie znaczenie tzw. „inżynierii wykrywania". Funkcje systemów EDR czy XDR prawdopodobnie staną się podstawową warstwą, na której działy IT mogą budować niestandardową logikę wykrywania, dostosowaną do własnego środowiska. W ostatnim czasie szczególnie dużą popularnością cieszą się na polskim rynku systemy EDR. Gartner przewiduje, że do końca 2025 r.

ponad 60 proc. klientów zastąpi starsze produkty antywirusowe połączonymi rozwiązaniami EPP i EDR. Warto w tym miejscu wyjaśnić, iż zasadnicza różnica pomiędzy produktami polega na tym, że EDR koncentruje się na aktywnym wykrywaniu zagrożeń, zaś EPP skupia się na zapobieganiu oraz identyfikacji zagrożeń w sposób pasywny. Poza tym EDR agreguje dane o zdarzeniach z punktów końcowych, zaś EPP oferuje w tym zakresie ograniczoną widoczność.

– Odnotowujemy, że popyt na produkty EPP w czystej formie minimalnie wzrasta, natomiast udział sprzedaży EDR rośnie gwałtownie. W większości przypadków EDR jest kupowany razem z EPP i w zasadzie możemy już stwierdzić, że te dwie kategorie produktów się łączą. W pewnym sensie EDR staje się specyficzną funkcją szerzej pojętej ochrony urządzeń końcowych – mówi Leszek Tasiemski, wiceprezes ds. badań i rozwoju w WithSecure.

W miarę rozprzestrzeniania się ataków, w tym również skierowanych przeciwko małym i średnim firmom, popyt na EDR-y powinien sukcesywnie rosnąć praktycznie w każdej grupie odbiorców biznesowych. Jednak w przypadku mniejszych firm poważnym wyzwaniem może być obsługa takich systemów, wymagająca specjalistycznej wiedzy technicznej.

– Klienci postrzegają EDR-y i XDR-y jako naturalny, wyższy poziom ochrony. Niemniej często w tym marketingowym szumie umyka fakt, że potrzebni są profesjonalni operatorzy, którzy potrafią wykorzystać potencjał tego rodzaju produktów. Wówczas użytkownicy mogą sobie niebawem uświadomić, że kupili technologię, której nie umieją spożytkować. W kolejnych latach będzie to szansa dla naszych partnerów handlowych, którzy na bazie EDR i XDR zapewnią klientowi usługi zarządzania – mówi Paweł Jurek, dyrektor ds. rozwoju w Dagma Bezpieczeństwo IT.

Jedną z kluczowych właściwości produktu zabezpieczającego jest blokowanie incydentów na punktach końcowych, a także zapobieganie ich rozprzestrzenianiu się w całej sieci. Za pomocą EDR-u można wykrywać anomalie i złośliwą aktywność w sieci, a także ustalać priorytety i analizować działania, które pomogą zespołowi bezpieczeństwa IT szybciej reagować na ataki. System ułatwia prowadzenie dochodzeń kryminalistycznych, dzięki centralnemu repozytorium danych pochodzących z wszystkich urządzeń końcowych (na tej postawie można prowadzić analizy). Nic dziwnego, że analitycy Gartnera określają EDR jako „nowy rodzaj technologii bezpieczeństwa", która pomaga wykrywać zagrożenia i reagować na nie w czasie rzeczywistym.

XDR, czyli czas na unifikację

Według raportu Enterprise Strategy Group, poświęconego systemom bezpieczeństwa, aż 66 proc. firm konsoliduje narzędzia, zaś 32 proc. planuje to zrobić w nieodległej przyszłości. Liczba urządzeń i aplikacji przyprawia o zawrót głowy szefów działów informatycznych. Mają oni coraz więcej trudności ➤

Zdaniem integratora

Grzegorz Świrkowski, CEO, Net Complex

Czynniki decydujące o wyborze rozwiązania do ochrony urządzeń końcowych są zróżnicowane i obejmują wiele aspektów. Jednym z kluczowych jest zrozumienie rodzajów cyberataków i zagrożeń, na które dana firma może się natknąć. To z kolei pomaga w dopasowaniu odpowiednich narzędzi i funkcji w celu skutecznej ochrony przed konkretnymi zagrożeniami. W procesie sprzedaży rozwiązań do ochrony urządzeń końcowych ważną rolę odgrywają resellerzy oraz integratorzy. Jako integrator dostarczamy kompletną usługę polegającą na dostarczeniu produktu, implementacji oraz szkolenia z obsługi. To podejście pomaga klientom przezwyciężyć obawy związane z nową technologią. Klienci często obawiają się, że niewłaściwe wdrożenie lub nieodpowiednie użytkowanie rozwiązania może zwiększyć ryzyko ataku, dlatego korzystanie z usług profesjonalnego integratora może zwiększyć ich pewność i zaufanie do określonego rozwiązania.

Karol Labe, CEO, Miecz Net

Małe i średnie firmy stosunkowo rzadko korzystają z takich systemów jak XDR, chociażby z uwagi na fakt, iż nie posiadają personelu zdolnego do obsługi tego rodzaju narzędzi. Natomiast odnotowujemy wzmożony popyt na rozwiązania typu EDR/XDR zwłaszcza ze strony sektora administracji rządowej. Ta grupa klientów korzysta ze specjalnych dotacji na bezpieczeństwo. O wyborze konkretnego rozwiązania decyduje zaufanie do danego producenta w kontekście jego podejścia do zarządzania samym rozwiązaniem. Duży wpływ na decyzje podejmowane przez klientów mają też rekomendacje resellerów.

związanych z zarządzaniem, korelacją danych, a także integracją kilkunastu, a w większych organizacjach kilkudziesięciu produktów pochodzących od różnych producentów.

– Zabezpieczenie punktów końcowych to tylko część ogólnej strategii bezpieczeństwa. Firmy postępują rozsądnie, jeśli wychodzą poza ten aspekt i dbają o ochronę całego środowiska. W idealnym scenariuszu jeden dostawca zapewnia współdziałające ze sobą rozwiązania gwarantujące spójną ochronę w całej firmowej sieci. Zapewnia to większe bezpieczeństwo, ogranicza administrację i obniża koszty – tłumaczy Stefan Fritz, Director Channel Sales na region Central EMEA w Sophosie.

Szansa na konsolidację pojawiła się wraz z debiutem się systemów XDR. Według Gartnera jest to narzędzie bazujące na SaaS, przeznaczone do wykrywania zagrożeń i reagowania na incydenty. XDR natywnie integruje wiele produktów zabezpieczających w spójny system operacyjny bezpieczeństwa. Nieco bardziej rozbudowana jest definicja Forrester Research. Według niej XDR ujednolica wykrywanie punktów końcowych istotnych dla bezpieczeństwa z telemetrią pochodzącą z narzędzi do analizy i widoczności sieci (NAV), poczty elektronicznej, zarządzania tożsamością i dostępem, jak też środowisk chmurowych. To platforma natywna dla chmury, zbudowana na infrastrukturze dużych zbiorów danych, zapewniająca zespołom ds. bezpieczeństwa elastyczność, skalowalność i możliwości automatyzacji. Przytoczone definicje są ważne, bowiem wielu dostawców próbuje interpretować XDR na swój sposób, dezinformując przy okazji potencjalnych klientów.

– Śmietnik informacyjny, który zawładnął rynkiem cyberbezpieczeństwa spowodował, że większość użytkowników nie potrafi realnie określić swoich potrzeb w relacji do rynkowej oferty dotyczącej wszelkiej maści „nowej generacji" systemów, usług i rozwiązań. To niezdecydowanie i zagubienie wykorzystują marketingowcy. Dochodzi do kuriozalnych sytuacji, kiedy mała firma dysponująca kilkoma komputerami składa zapytanie ofertowe jak na wahadłowiec – mówi Grzegorz Michałek, CEO Arcabitu.

Jakby nie patrzeć XDR, jak sama nazwa wskazuje, jest rozszerzeniem systemu EDR. Chociaż EDR umożliwia szybkie reagowanie, to może skupiać się jedynie na punktach końcowych, podczas gdy XDR koncentruje się szerzej na wielu punktach kontroli bezpieczeństwa, wykorzystując wielkie zbiory danych, głęboką analizę i automatyzację. To ważny krok w kierunku unifikacji. Jednak trzeba mieć na uwadze, że nie ma nic za darmo.

– Zunifikowane platformy dają wartość w postaci łatwiejszego zarządzania całością, ale wiąże się to z kompromisem, którym może być utrata możliwości korzystania z zaawansowanych funkcji – przestrzega Paweł Jurek. ■

Zdaniem specjalisty

Stefan Fritz, Director Channel Sales Central EMEA, Sophos

Z naszego raportu „State of Ransomware 2023" wynika, że w ciągu minionego roku 68 proc. firm padło ofiarą cyberataku. Dlatego nowoczesna ochrona powinna być podstawą każdej skutecznej strategii bezpieczeństwa, co jednak nie wystarcza. Cztery na pięć przedsiębiorstw przyznaje, że ich zespoły IT mają niedobory w zakresie specjalistycznej wiedzy na temat bezpieczeństwa. Z pomocą przychodzą im rozwiązania zapewniające pełny wgląd w to, jak zagrożenia dostają się do sieci oraz co jest celem hakerów. W zwiększaniu bezpieczeństwa klientów ważną rolę odgrywa sprzedaż kanałowa. Dostarczane im przez partnerów informacje, szkolenia i specjalistyczna wiedza odgrywają kluczową rolę przy projektowaniu systemów cyberbezpieczeństwa.

Grzegorz Michałek, CEO, Arcabit

Uczenie maszynowe w branży cyberbezpieczeństwa jest wykorzystywane od dawna. Przynosi ono realne korzyści wszystkim zainteresowanym stronom w postaci automatyzacji i przyspieszania analizy ogromnych zbiorów danych, chociażby takich jak kolekcja szkodliwych plików, skryptów, wiadomości czy stron internetowych.

Nieco inaczej wygląda to w przypadku sztucznej inteligencji, która z tradycyjnie rozumianą inteligencją ma niewiele wspólnego. Eksplozywny wzrost popularności tego zjawiska nie wpłynął znacząco na funkcjonowanie laboratoriów i działów deweloperskich producentów. Oni dalej robią swoje. Natomiast potencjał drzemiący w ogólnoświatowym zachwycie AI błyskawicznie dostrzegły i włączyły do swojego repertuaru działy promocji i sprzedaży. Silniejszą pozycję w tej rywalizacji w oczywisty sposób zajmują cyberprzestępcy, ponieważ to oni mają stały dostęp do oferowanych przez producentów rozwiązań i mogą przygotowywać ataki w taki sposób, aby najnowsze wersje pakietów i usług ochronnych nie blokowały pierwszej fali kampanii hakerskich. Oczywiście producenci nie są tutaj bezbronni, jednak wymaga to faktycznego zaangażowania w rozwój oprogramowania.

Paweł Jurek, Business Development Director, Dagma Bezpieczeństwo IT

Obserwujemy wśród klientów intensywne przechodzenie od rozwiązań najprostszych do bardziej złożonych pakietów, umożliwiających korzystanie z rozbudowanych funkcji bezpieczeństwa. W segmencie firm małych i średnich oznacza to zaawansowaną ochronę antywirusową z wykorzystaniem sandboxingu. Taki poziom ochrony zapewnia wysoki poziom bezpieczeństwa przy zachowaniu prostoty zarządzania. Firmy większe, ale też wsparte dofinansowaniem instytucje samorządowe i rządowe, mocno inwestują w funkcji EDR/XDR, gdzie trzeba już mieć ekspertów dających sobie radę z obsługą incydentów bezpieczeństwa. Klienci korporacyjni, którzy chcą skorzystać ze zintegrowanego zarządzania, mają do dyspozycji szeroką paletę funkcji. Pozostaje im wybór dotyczący tego, czy będą taką ochroną chcieli zarządzać sami, czy może wyznaczą tę rolę zaufanemu partnerowi.

ESET: czas na Elite!

ESET PROTECT Elite to antidotum na cyberataki, zapewniające skuteczną, wielowarstwową ochronę infrastruktury średnich i dużych firm.

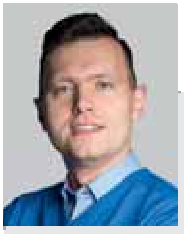
Unijni prawodawcy stawiają firmom i instytucjom coraz to nowe wymogi prawne w dziedzinie ochrony przed cyberatakami. Jednak wiele organizacji zwleka z przystosowaniem się do nich do ostatniej chwili. Kłopoty mogą mieć w związku z tym firmy, które zbyt późno uświadomią sobie, że one też muszą wdrożyć odpowiednie procedury oraz narzędzia, aby móc działać zgodnie z przepisami i tym samym uchronić się przed wysokimi karami.

Obecnie wielu przedsiębiorców boryka się z dyrektywą NIS2. Jak się okazuje, muszą się do niej dostosować nie tylko podmioty klasyfikowane jako kluczowe bądź istotne, ale również te, które z nimi współpracują (np. będąc jednym z ogniw w łańcuchu dostaw). A z tego wniosek, że może to dotyczyć nawet niedużych firm.

Niestety, czas nie działa na ich korzyść – termin implementacji przepisów dyrektywy NIS2 mija 17 października 2024 r. Palącą staje się zatem kwestia znalezienia rozwiązań, które są szybkie we wdrożeniu, łatwe w użytkowaniu i zarządzaniu, a ponadto o możliwie najszerszym wachlarzu funkcji ochronnych, które stanowią skuteczną odpowiedź na wciąż zmieniający się krajobraz cyberzagrożeń.

To dobry moment dla partnerów DAGMA Bezpieczeństwo IT na przedstawienie klientom pakietu ESET PROTECT Elite, który zapewnia kompleksową ochronę przed cyberatakami średnim i dużym firmom. Obejmuje działaniem stacje robocze, serwery, urządzenia mobilne, pocztę, współpracę i przechowywanie danych w chmurze. Oferuje rozwiązania maksymalizujące ochronę, jak XDR, uwierzytelnianie wieloskładnikowe i funkcję zarządzania podatnościami.

Funkcjami pakietu zarządza się przez konsolę ESET PROTECT. Zapewnia ona w czasie rzeczywistym informacje na temat wszystkich urządzeń, a także pełne raportowanie i zarządzanie bezpieczeństwem wszystkich systemów operacyjnych. Można ją wdrożyć w chmurze lub lokalnie, a sam pakiet Elite partnerzy mogą oferować klientom w modelu Managed Service Provider.



Bartosz Różalski,
Senior Product Manager ESET,
DAGMA Bezpieczeństwo IT

Dostosowywanie do wymogów dyrektywy wymaga aktualizacji lub nawet opracowania od nowa procedur, które są realizowane przez pracowników danej organizacji lub zespół IT. Do realizacji wytycznych niezbędne będą odpowiednie narzędzia, wspierane przez dział IT lub dział bezpieczeństwa. Przy czym firmy mogą powierzyć zewnętrznym dostawcom obsługę incydentów w modelu abonamentowym. Dlatego elastyczna oferta ESET wpisuje się w zmieniające się potrzeby przedsiębiorstw i umożliwia partnerom realizację umów na warunkach, które będą dopasowane do preferencji i korzystne dla klientów.

Pakiet ESET PROTECT Elite zawiera następujące funkcje:

- **ochrona stacji roboczych** – umożliwia wielopoziomową ochronę komputerów i smartfonów dzięki technologii Eset LiveSense; zabezpiecza przed złośliwym oprogramowaniem, blokuje ukierunkowane ataki, zapobiega naruszeniom bezpieczeństwa danych, zatrzymuje ataki bezplikowe;
- **ochrona systemów serwerowych** – chroni w czasie rzeczywistym wszystkie dane firmy przetwarzane na serwerach plików; zapobiega atakom ransomware, wykrywa zagrożenia zero-day, zapobiega naruszeniom bezpieczeństwa danych, chroni przed botnetami;
- **pełne szyfrowanie dysków** – zaawansowane rozwiązanie do pełnego szyfrowania dysku, w celu zapewnienia zgodności z obowiązującymi przepisami;
- **sandboxing w chmurze** – zapewnia proaktywną ochronę przed zagrożeniami typu zero-day oraz przed nowymi zagrożeniami, wykorzystując uczenie maszynowe i analizę behawioralną;
- **ochrona aplikacji** w chmurze – zapewnia zaawansowaną ochronę aplikacji platformy Microsoft 365 przed złośliwym oprogramowaniem, spamem i atakami typu phishing oraz ochronę przed zagrożeniami zero-day; rozwiązanie to jest wyposażone w specjalną konsolę zarządzania w chmurze;
- **bezpieczeństwo poczty e-mail** – blokuje wszystkie ataki wykorzystujące złośliwe oprogramowanie, spam, ataki typu phishing na poziomie serwera pocztowego, zanim dotrą do skrzynek pocztowych użytkowników;
- **zarządzanie podatnościami (nowość)** – to funkcja śledzenia i usuwania luk w zabezpieczeniach systemów operacyjnych i aplikacji na różnych rodzajach stacji roboczych; chroni przed zagrożeniem ze strony nieaktualnych systemów operacyjnych i aplikacji;
- **Extended Detection & Response (XDR)** – rozbudowane funkcje konsoli Eset PROTECT o komponent klasy XDR, który pozwala przeciwdziałać naruszeniom, umożliwia dogłębną analizę zagrożeń oraz sposobów zapobiegania im;
- **uwierzytelnianie wieloskładnikowe** – szybka do wdrożenia i zarządzana przez internet funkcja wykorzystująca aplikację mobilną, która chroni firmę przed używaniem słabych haseł i nieupoważnionym dostępem.

eset DAGMA BEZPIECZEŃSTWO IT

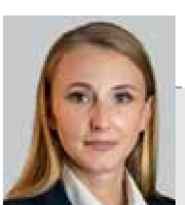
Więcej informacji:
Bartosz Różalski, Senior Product Manager ESET w DAGMA Bezpieczeństwo IT
rozalski.b@dagma.pl

Fortinet: zautomatyzowana ochrona przed zaawansowanymi zagrożeniami

W czasach, gdy cyberataki stają się coraz bardziej zaawansowane i nieprzewidywalne, konieczne jest stosowanie najnowocześniejszych rozwiązań ochronnych – nie tylko dla sieci, ale także dla urządzeń końcowych.

Już od paru lat możliwe jest zwiększenie poziomu ochrony urządzeń końcowych w przedsiębiorstwach dzięki nowej klasie narzędzi, wykraczających swoją skutecznością i funkcjonalnością daleko poza klasyczne antywirusy. Oprogramowanie typu EDR (Endpoint Detection and Response) wykrywa zaawansowane zagrożenia, takie jak bezplikowe złośliwe oprogramowanie czy ransomware i zapewnia reagowanie w czasie rzeczywistym, wspomagane przez uczenie maszynowe. Z kolei XDR (Extended Detection and Response) dodatkowo łączy dane o zagrożeniach z wielu źródeł, w tym urządzeń końcowych, sieci i środowisk chmurowych oraz wykorzystuje zaawansowaną analitykę i sztuczną inteligencję do wykrywania ataków i reagowania na nie.

Do tego typu narzędzi należą FortiEDR oraz FortiXDR firmy Fortinet. Umożliwiają one przedsiębiorstwom wdrażanie zaawansowanych oraz spójnych strategii reagowania na zagrożenia, a także budowania cyfrowej odporności.



Agnieszka Szarek,
Distribution Sales Manager, Fortinet

Serdecznie zapraszamy do kontaktu wszystkich integratorów zainteresowanych rozwiązaniami z kategorii XDR/EDR do ochrony urządzeń końcowych. Z przyjemnością przedstawimy funkcjonalność produktów Fortinet oraz ich wyróżniki konkurencyjne. Partnerzy rozpoczynający współpracę z nami mogą liczyć na dostęp do szkoleń, jak również na wsparcie opiekuna przy realizacji pierwszych wdrożeń. Gwarantujemy też atrakcyjny system rabatów i marży, aby nasza współpraca była korzystna dla wszystkich stron.

Fot. Adobe Stock

Błyskawiczna analiza i reakcja

Jedną z kluczowych funkcji rozwiązania **FortiEDR** jest zdolność do identyfikowania nowych zagrożeń, które mogą ominąć tradycyjne metody zabezpieczania. Odbywa się to dzięki zaangażowaniu sztucznej inteligencji do analizy ruchu sieciowego, zachowania użytkowników oraz innych czynników, które mogą wskazywać na niebezpieczeństwo. Głównym celem jest minimalizacja czasu reakcji na ataki, co pozwala ograniczyć potencjalne straty wskutek groźnego incydentu.

W przypadku wykrycia potencjalnego zagrożenia FortiEDR jest w stanie natychmiast zareagować poprzez odizolowanie zainfekowanego urządzenia od reszty infrastruktury oraz rozpoczęcie analizy w środowisku testowym sandbox, zapewnianym przez usługę chmurową Fortinet Cloud. Pozostali pracownicy mogą kontynuować wykonywanie służbowych obowiązków, a więc nie dochodzi do paraliżu całej firmy. Wykorzystanie sztucznej inteligencji i mechanizmów uczenia maszynowego przyczynia się też do minimalizowania liczby fałszywych alarmów.

Po zakończeniu śledztwa i ewentualnych napraw administratorom dostarczany jest obszerny raport z analizą anomalii. Dzięki niemu zyskują oni możliwość zrozumienia źródła zagrożenia i opracowania strategii zapobiegania przyszłym atakom. Mimo zaawansowanej funkcjonalności, FortiEDR oferuje korzystny stosunek jakości do ceny, co jest szczególnie ważne dla klientów dysponujących ograniczonym budżetem.

Zintegrowany ekosystem ochronny

Rozwiązanie **FortiXDR** jest narzędziem, które oferuje przedsiębiorstwom szerszy zakres funkcji niż tradycyjne rozwiązania EDR. Zapewniają one wykrywanie zagrożeń, analizowanie ich i reagowanie na nie w sposób bardziej holistyczny. XDR stanowi swego rodzaju hub informacji dotyczących incydentów bezpieczeństwa.

Przy czym, żeby skuteczność analizy zagrożeń była jak największa, zapewniona została kompatybilność FortiXDR z innymi narzędziami stworzonymi przez Fortinet (takimi jak firewalle FortiGate czy systemy FortiSIEM), połączonymi ze sobą w ramach architektury Fortinet Security Fabric. Rozwiązania te wymieniają się informacjami o podejrzanych sytuacjach w czasie rzeczywistym, tworząc spójny ekosystem bezpieczeństwa, zapewniający lepszą widzialność poziomu ochrony całego środowiska IT.

Podobnie jak w przypadku FortiEDR, sztuczna inteligencja zapewnia bardzo szybkie wykrywanie zaawansowanych ataków w urządzeniach końcowych oraz sieci. Reagowanie na nie jest zautomatyzowane, co pozwala na błyskawiczne izolowanie zainfekowanych urządzeń oraz minimalizację potencjalnych szkód, a tym samym zwiększenie efektywności w zarządzaniu zagrożeniami i ochroną danych. FortiXDR zastępuje pracę wykonywaną przez wyspecjalizowanych ekspertów, więc jest idealnym narzędziem dla przedsiębiorstw borykających się z niedoborem personelu.

Kontakt dla partnerów:
Agnieszka Szarek,
Distribution Sales Manager, Fortinet
aszarek@fortinet.com

G DATA academy

12345

W sam raz jako miesięczna wypłata.
Zdecydowanie nie jako hasło.

G DATA Security Awareness Trainings
Cyberbezpieczeństwo zaczyna się od pracowników. Jeśli personel jest przygotowany i zna możliwe zagrożenia, znacznie zmniejsza to ryzyko kosztownych ataków.

Wzmocnij ludzki firewall swoich klientów ze szkoleniami G DATA!
Sprawdź na https://gdata.pl/szkolenia

Tehtris: pełna automatyzacja cyberochrony

Tehtris XDR Platform to rozwiązanie cyberbezpieczeństwa, które już teraz jest gotowe na nadchodzące zagrożenia IT.

Obecny od niedawna na polskim rynku francuski producent Tehtris specjalizuje się w zautomatyzowanym neutralizowaniu cyberataków. Jego flagowe rozwiązanie Tehtris XDR Platform to jedyna w pełni europejska platforma eliminująca cyberataki w czasie rzeczywistym. Rozwiązania tej marki funkcjonują w ponad 100 krajach, w takich branżach jak przemysł, transport, ochrona zdrowia, administracja publiczna czy infrastruktura krytyczna. Do grona ich użytkowników należą między innymi Michelin, Alstom, Orange czy Somfy.

Tehtris stawia na technologie budowane wewnątrz firmy i pełną integrację oraz współdziałanie wszystkich składników ochrony w ramach autorskiej platformy XDR. Oferta marki jest kompletna i obejmuje: wykrywanie, reagowanie oraz ochronę na punktach końcowych (EDR+EPP); zabezpieczanie urządzeń mobilnych (MTD); gromadzenie, korelowanie i analizę alertów spływających z chronionej sieci, łącznie z wykrywaniem anomalii w zachowaniu użytkowników (SIEM); rozbudowaną analizę ruchu sieciowego, także w modelu zerowego zaufania (NTA oraz ZTNA) czy wreszcie mechanizm pozwalający na automatyzację całego arsenału cyberbezpieczeństwa, a także wdrażanie rozbudowanych scenariuszy ochrony oraz reagowania (SOAR).

Należy podkreślić, że wszystkie komponenty ochrony są wspierane przez autorską technologię sztucznej inteligencji, która jest w stanie nie tylko wykrywać nieznane cyberataki, ale także kategoryzować alerty i podejmować autonomiczne działania naprawcze. Rozwiązania Tehtris nie przesyłają do chmury żadnych danych użytkowników. Trafiają tam jedynie sumy kontrolne, które nigdy nie opuszczają terytorium Unii Europejskiej.

Tehtris wychodzi z założenia, że firmy potrzebują rozwiązania cyberbezpieczeństwa, które automatycznie neutralizuje wszelkie zagrożenia bez interakcji człowieka już na wstępnym etapie ataku. Innymi słowy, należy powstrzymać atakujących zanim zdążą wyrządzić jakiekolwiek szkody. Z kolei analitycy z działów SOC oraz zespoły reagujące na incydenty potrzebują przefiltrowanych alertów z nadanymi priorytetami, jako że nie są w stanie zajmować się ręcznie każdym ostrzeżeniem. Sposobem na ułatwianie prowadzenia prac w zakresie kryminalistyki cyfrowej jest przechowywanie dzienników zdarzeń oraz danych telemetrycznych i oferowanie zaawansowanych narzędzi analitycznych (wraz z szybkim wyszukiwaniem).

Autoryzowanym przedstawicielstwem firmy Tehtris na terenie Polski jest spółka DLP Expert z siedzibą w Warszawie. Klienci oraz firmy zainteresowane współpracą mogą liczyć na atrakcyjne ceny przygotowane specjalnie z myślą o rynku polskim oraz na pomoc zespołu DLP Expert w zakresie wdrożeń, a także prezentacji sprzedażowych i technicznych.

Szczegółowe informacje o rozwiązaniach Tehtris są dostępne na stronie https://dlp-expert.pl/tehtris.

Sztuczna inteligencja w cenie

Jedną z cech wyróżniających portfolio Tehtris jest bogaty zestaw zaawansowanych technologii oferowanych bez dodatkowych opłat wraz z rozwiązaniem Tehtris XDR Platform. Należą do nich:

- Technologia SOAR (Security Orchestration, Automation and Response) ułatwiająca automatyzację zadań związanych z cyberbezpieczeństwem, z wykorzystaniem predefiniowanych oraz własnych scenariuszy.
- Moduł CTI (Cyber Threat Intelligence) – nieustannie uaktualniany cyfrowy magazyn eksperckiej wiedzy o cyberzagrożeniach. CTI oferuje dostęp do narzędzi umożliwiających błyskawiczną analizę podejrzanych plików w odizolowanym środowisku (sandbox) i umożliwia aktywne wyszukiwanie nowych zagrożeń.
- Autorska technologia sztucznej inteligencji Cyberia, zdolna do wykrywania oraz neutralizowania nieznanych cyberzagrożeń i wspomagająca zautomatyzowaną analizę oraz neutralizację incydentów bezpieczeństwa.
- Analiza danych związanych z cyberbezpieczeństwem w chronionej sieci - dostęp do wszystkich danych o bezpieczeństwie zgromadzonych w infrastrukturze klienta do sześciu miesięcy wstecz.
- Możliwość przeprowadzania audytu cyberbezpieczeństwa w chronionej sieci.

Kontakt dla partnerów
DLP Expert, ul. Trawiasta 35, 04-607 Warszawa
info@dlp-expert.pl,
tel. 22 299 22 09, 22 299 45 46,
https://dlp-expert.pl

Stormshield: wodociągowe studium przypadku

Inżynierowie Stormshielda zadbali, aby zgodność z nowymi unijnymi regulacjami, w kontekście separacji i monitorowania sieci OT, nie przysporzyła integratorom większego kłopotu.

Zbliżająca się implementacja dyrektywy NIS2 nałoży nowe obowiązki nie tylko na duże, ale również na mniejsze podmioty. Aby to lepiej zobrazować, posłużymy się przykładem jednego z wdrożeń, jakie miały miejsce w firmie wodno-kanalizacyjnej z północnej części Polski. Przy czym od razu trzeba podkreślić, że specyfiką działalności podmiotów z tego sektora jest odseparowanie poszczególnych części systemu – punktów ujęcia wody, jej uzdatniania czy przepompowni ścieków – co zwiększa ryzyko ataku. Jednocześnie efektywne zarządzanie nimi odbywa się w coraz większym stopniu w oparciu o dostęp online.

Celem omawianego projektu było wdrożenie solidnego rozwiązania w zakresie bezpieczeństwa sieci, które skutecznie oddziela i zabezpiecza sieci operacyjne (OT) od sieci informatycznych (IT) w wielu lokalizacjach – przepompowniach i ujęciach wody. Strategia trwającego około miesiąca projektu obejmowała separację sieci w oparciu o firewalle Stormshield SNi20 na obrzeżach każdej z sieci OT.

Wybór lokalizacji zapór został oparty na rygorystycznej ocenie ryzyka i działających już połączeniach sieciowych. Urządzenia zostały umieszczone jak najbliżej urządzeń automatyki przemysłowej, często na tej samej szynie DIN, co sterowniki PLC. Ułatwia to szybkie wykrywanie zagrożeń i reagowanie na nie. Minimalizuje przy tym powierzchnię ataku i maksymalizuje ochronę infrastruktury przemysłowej.

Zamiast wprowadzać znaczące zmiany w topologii sieci, rozwiązanie Stormshield wykorzystuje interfejsy w konfiguracji bridge do segmentacji. Technika ta pozwala na izolację różnych segmentów przy zachowaniu ogólnej struktury sieci. Ogranicza to zakres wymaganych modyfikacji, zmniejszając ryzyko zakłóceń operacyjnych.

Znaczenie miała również centralizacja zapewniająca, że tylko autoryzowane urządzenia i podmioty mogą wchodzić w interakcje z krytycznymi zasobami, minimalizując potencjalną powierzchnię ataku. Dzięki wykorzystaniu SMC, zmiennych i możliwości oskryptowania łatwo zarządzać, zmieniać politykę i aktualizować centralnie wszystkie podłączone firewalle SNi20 i EVA, mimo że cechuje je indywidualna polityka w każdej lokalizacji.

Kontrola odbywa się w ramach standardowych prac konserwatorskich i nastawczych. Pierwszorzędne znaczenie ma autoryzacja pracowników z użyciem istniejących Active Directory i integracji poprzez mechanizm SSO. Następnie monitorowane i zapisywane są wszystkie działania w ramach protokołów przemysłowych, przepuszczanych na urządzeniach. Zdarzenia są rejestrowane w centralnym systemie SIEM, a całość zarządzana z centralnego systemu Stormshield Management Center.

Wymogi NIS2 pod kontrolą

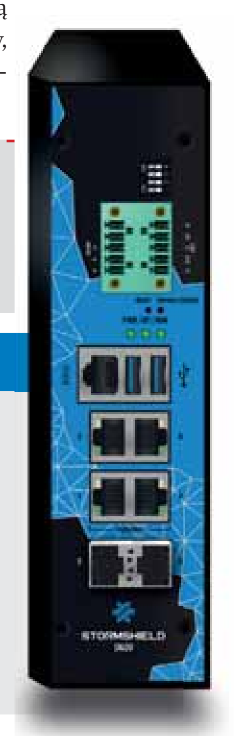
Dyrektywa NIS2 wprowadza obowiązki stosowania określonych środków ochrony oraz szereg wymogów, np. raportowanie incydentów naruszenia bezpieczeństwa, zapewnienie odpowiedniego poziomu bezpieczeństwa produktów i przekazywania informacji o zagrożeniach i wadach. Dyrektywa wprowadza przy tym dwie kategorie podmiotów – kluczowych i istotnych – wobec których obowiązki są zróżnicowane. Obejmują zgłaszanie incydentów i zagrożeń, zarządzanie kryzysowe, opracowanie odpowiednich polityk oraz procedur testowania i audytów, a także stosowanie rozwiązań technologicznych adekwatnych do ryzyka.

Powyższe oznacza, że wdrożenie rekomendowanych rozwiązań będzie czasochłonne, a wobec skali wyzwania nawet uwzględnienie czasu przewidzianego w vacatio legis może okazać się niewystarczające. Tym bardziej stosowanie już teraz adekwatnych do ryzyka mechanizmów ochronnych jest dobrym posunięciem. Zwłaszcza, że podmioty, które nie będą przestrzegać dyrektywy, mogą być ukarane między innymi grzywnami.

Kontakt dla partnerów:
Piotr Zielaskiewicz, Senior Product Manager w DAGMA Bezpieczeństwo IT
zielaskiewicz.p@dagma.pl

Osiągnięte główne cele projektu to...

- **Separacja** – skutecznie oddzielono sieci OT od sieci IT przy pomocy firewalli SNi20, minimalizując ryzyko zagrożeń z wewnętrznej sieci IT.
- **Centralizacja** – każdy firewall SNi20 w konfiguracji bridge, pomimo wspólnych cech ma niestandardową politykę bezpieczeństwa, która kontroluje dostępy do wyznaczonych zasobów w segmencie.
- **Bezpieczeństwo** – monitorowanie w czasie rzeczywistym przy pomocy systemu SIEM i scentralizowane zarządzanie firewallami brzegowymi z pomocą SMC przyspiesza reakcję i rekonfigurację.
- **Zgodność z przepisami** – anonimizacja danych osobowych zgodnie z wytycznymi RODO.
- **Ulepszona ochrona SCADA** – wirtualny firewall EVA zapewnia dodatkową warstwę zabezpieczeń do systemów SCADA.
- **Niezawodność** – firewalle SNi20 mają możliwość funkcji bypass, co oznacza ciągłość transmisji.



Fot. Adobe Stock

Chmura i usługi w programach partnerskich

Model usługowy wymusza zmianę benefitów, szkoleń, modelu rozliczeniowego, a nawet statusów partnerskich. Co ważne, w ramach nowego podejścia, producenci oczekują od integratorów większej samodzielności.

■ *Krzysztof Pasławski*

Najważniejsze dla dobrej współpracy producentów i ich partnerów są: przewidywalność, transparentne reguły gry, jasne zasady ochrony projektów, transfer wiedzy, bonusy i profity, jak też wsparcie projektowe oraz przed i posprzedażowe. Co istotne, oprócz samych zasad współpracy, nie mniej ważne są „miękkie" aspekty relacji, o ile ma być ona korzystna dla każdej ze stron. Współpraca, jak to w biznesie, wręcz musi być oparta na wzajemnym zaufaniu, bez czego nie będzie ani trwała, ani owocna. Dlatego przy rozważaniach na ten temat nie można pominąć dużego znaczenia tzw. czynnika ludzkiego.

Programy ewoluują w kierunku większej personalizacji.

– *Bardzo ważną rolę odgrywa bezpośredni kontakt, nie tylko poprzez mejle i telefony, ale również spotkania i indywidualne konsultacje z opiekunem handlowym* – mówi Krzysztof Mertowski, Head of Sales w polskim oddziale Brothera.

Rzecz jasna, dobre programy partnerskie to takie, które zmieniają się zgodnie z potrzebami i możliwościami wszystkich zainteresowanych stron.

– *Tym, co niewątpliwie doceniają partnerzy – poza aspektami ekonomicznymi, jak rabaty, prowizje, bonusy – jest elastyczność programów partnerskich, wsparcie edukacyjne producenta i jego gotowość do zmian, a także wprowadzanie innowacyjnych rozwiązań i możliwość budowania długotrwałych relacji, które przekładają się na jakość współpracy* – twierdzi Błażej Kowalkiewicz, Field & Channel Marketing Manager CEE w Vertivie.

Jednocześnie wszyscy producenci są zgodni co do znaczenia poszerzania wiedzy przez partnerów, zwłaszcza na tak zmiennym rynku, z jakim mamy ostatnio do czynienia. Przy czym szkolenia czy warsztaty powinny realnie pomagać firmom z kanału sprzedaży w rozwoju działalności.

– *Partnerzy bardzo doceniają wszelkie aktywności wspierające rozwój kompetencji i ich użycie w generowaniu nowych szans biznesowych. Nie bez znaczenia jest także wskazywanie kierunków rozwoju oferty na obszary, w które partnerzy powinni inwestować, aby zwiększać swoją konkurencyjność i atrakcyjność w oczach klientów* – mówi Dariusz Okrasa, Senior Channel Sales Manager w Dell Technologies.

Certyfikaty nie są do ramki

Z poszerzaniem kompetencji wiążą się certyfikaty, które są wymagane właściwie w każdym programie partnerskim. Z punktu widzenia integratorów bardzo ważne jest, aby certyfikacje stanowiły dla nich wyróżnik oraz wiązały się z wymiernymi korzyściami.

– *Certyfikat, żeby przedstawiał wartość dla partnera, powinien być wyróżnikiem dla tych najbardziej zaangażowanych, którzy zainwestowali swój czas i pieniądze, aby promować daną markę* – podkreśla Przemysław Biel, Sales Channel Manager Poland w Synology.

Takim wyróżnikiem może być chociażby polecanie klientom certyfikowanych partnerów i przekazywanie certyfikowanym integratorom leadów, które spływają bezpośrednio do producenta. Przy czym istotne jest, aby konkretne korzy-

Fot. Adobe Stock

ści były dostępne nie tylko na wyższych poziomach współpracy. Konieczna jest również przejrzystość – jasne zasady i benefity, które partner osiąga przez swoją aktywność.

– *Program partnerski powinien być tak zaprojektowany, aby dawał korzyści na każdym etapie zaangażowania partnera w daną markę. Jeśli dopiero zaczyna, to oczywiście nie dostaje największych benefitów, ale musi mieć jasno określoną ścieżkę, jak może do nich dotrzeć* – podkreśla Przemysław Biel.

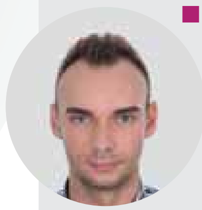
Przesuwanie „dźwigni"

W ostatnich latach można było zaobserwować postępującą ewolucję programów. Producenci kładą coraz większy ➤

Zdaniem specjalisty

Marcin Gwara, Channel Manager, Fujitsu

Partner musi przede wszystkim czuć wsparcie producenta w ochronie projektów. Moment, w którym dochodzi do rejestracji projektu, jest bardzo istotny. To element budowania zaufania między nami, który rzutuje na całą współpracę. Dlatego uważam, że jasne i przejrzyste zasady ochrony projektów są kluczem do udanego partnerstwa. Drugim aspektem jest transfer wiedzy. Partner, który posiada odpowiednie kompetencje, czuje się o wiele bardziej niezależny i gotowy do podejmowania większych wyzwań, jakie mogą stawiać klienci. Trzecim elementem jest gratyfikacja, czyli program lojalnościowy, który będzie motywował i dawał partnerowi odczuć, jak istotna jest jego rola.



Błażej Kowalkiewicz, Field & Channel Marketing Manager CEE, Vertiv

Wraz z rozwojem chmury i usług zarządzanych partnerzy muszą rozwijać nowe umiejętności, takie jak zarządzanie usługami w chmurze, integracja różnych rozwiązań cloud czy zapewnienie bezpieczeństwa w chmurze. Wraz z rozwojem cloud computingu i modelu as-a-service rynek stał się bardziej konkurencyjny. Partnerzy muszą dostarczać większą wartość dodaną, taką jak specjalistyczne usługi, doradztwo czy wsparcie, aby wyróżnić się na tle konkurencji. Z drugiej strony obserwujemy, że producenci (nie tylko ci z branży IT) nie skupiają się wyłącznie na sprzedaży – ich nowoczesne programy partnerskie kładą nacisk na dostarczanie wartości dodanej. Może to obejmować edukację, wsparcie techniczne czy dostęp do ekskluzywnych zasobów – sklepów z nagrodami.

Dariusz Okrasa, Senior Channel Sales Manager, Dell Technologies

Program partnerski powinien być jak dobrze skrojony garnitur. Ma jak najlepiej pasować do specyfiki biznesu partnera i nagradzać zaangażowanie. Mam tu na myśli potrzeby resellerów, dystrybutorów, integratorów czy partnerów dostarczających rozwiązania w modelu usługowym. Program ewoluuje, aby odpowiadać na trendy rynkowe, takie jak multicloud, AI, edge computing czy IoT, i pozostawia partnerom dużą swobodę w inwestowaniu w najlepiej odpowiadające im kierunki. Obserwujemy, że wielu typowo transakcyjnych partnerów sięga po zaawansowane produkty, monetyzując w ten sposób inwestycje w nowe kompetencje. Kładziemy duży nacisk na samodzielność partnerów w podejmowaniu decyzji o zaangażowaniu w poszczególne segmenty portfolio i programy Della, co przekłada się na dochodowość tej współpracy.

Krzysztof Mertowski, Head of Sales, Brother

Ze względu na utrzymującą się na rynku niepewność gospodarczą, partnerzy oczekują przede wszystkim marży, która zapewni im „bezpieczeństwo biznesowe". Programy partnerskie i zasady współpracy powinny być tak skonstruowane, aby umożliwiały firmom rozwój, a nie go hamowały. Przykładem takich sytuacji są skomplikowane umowy, długie terminy oczekiwania na produkty lub nieobliczalne promocje, które prowadzą do niepotrzebnej frustracji. Wyjściem z sytuacji są transparentne warunki współpracy oraz dedykowane programy zarówno dla sklepów internetowych, ale również firm, które wykonują aktywną sprzedaż, uwzględniając wsparcie techniczne. Ważnym elementem pomocy partnerom są również szkolenia i certyfikaty, które pozwalają uzyskiwać najlepsze statusy u producenta.

nacisk na samodzielność ze strony partnerów. Chodzi o swobodę w rozwoju oferty w oparciu o różne dostępne rozwiązania, platformy bądź model subskrypcyjny. Z drugiej strony za bardzo korzystne należy uznać wszelkie działania w drugą stronę, a więc dostosowywanie się vendorów do potrzeb integratorów. Dobrym przykładem jest Fujitsu.

– *Chcemy przesunąć dźwignię z miejsca, w którym partner na podstawie portfolio vendora buduje swoją ofertę, w stronę dostosowania naszego portfolio pod potrzeby partnera. I tutaj pojawia się największe wyzwanie, jakim jest wzajemne zaufanie i otworzenie się na rozmowę w układzie innym niż producent-sprzedawca. Często ten układ zamieniamy tak, że to partner staje się dostawcą dla nas* – mówi Marcin Gwara, Channel Manager w Fujitsu.

Programy partnerskie ewoluują w kierunku większej personalizacji – dostosowywania współpracy do indywidualnych potrzeb i konkretnych partnerów – między innymi za pomocą technologii (automatyki marketingowej, CRM-ów, narzędzi do analizy danych).

– *Te technologie umożliwiają lepsze śledzenie wyników, automatyzację procesów i bardziej spersonalizowane podejście do partnerów. Dzięki nim programy partnerskie są coraz bardziej dostosowywane do indywidualnych preferencji firm współpracujących. Ponadto warto zaznaczyć, że w obecnych czasach programy partnerskie nie ograniczają się tylko do jednego kanału. Obejmują one różne kanały, w tym programy poleceń oraz partnerstwa strategiczne* – zapewnia Błażej Kowalkiewicz.

Kolejną ważną zmianą, w tym przypadku dla integratorów działających na rynku druku, staje się dostosowanie programu partnerskiego do rozwoju sprzedaży w internecie, gdzie przeniosła się również ze swoimi zakupami spora część klientów biznesowych.

Z punktu widzenia partnerów duże znaczenie mają…

- **…wzajemne korzyści** – program powinien być zaprojektowany tak, aby obie strony czerpały z niego profity w zależności od stopnia zaangażowania;
- **…wsparcie i szkolenia** – wsparcie dla partnerów na każdym etapie projektu, a także przed- i posprzedażowe, jak też szkolenia online i stacjonarne;
- **…komunikacja** – regularna, otwarta i przejrzysta pomiędzy partnerem a producentem;
- **…technologia** – udostępnianie takich narzędzi jak platformy partnerskie, systemy rejestracji projektów, a nawet aplikacje wykorzystujące VR (pomagają partnerom w prezentacji rozwiązań klientom);
- **…jasne warunki współpracy** – umowy powinny być precyzyjne i sprawiedliwe, obejmując przede wszystkim ochronę zarejestrowanego projektu oraz sposoby naliczania i wysokość rabatów;
- **…elastyczność i stałe monitorowanie** – program partnerski powinien być dostosowywany do zmian na rynku i odpowiadać na bieżące potrzeby partnerów;
- **…motywowanie do dalszej współpracy** – rabaty, bonusy za osiągnięcia i inne formy motywacji poprawiają zaangażowanie partnerów.

Błażej Kowalkiewicz, Field & Channel Marketing Manager CEE, Vertiv

Programy dla chmury i usług

Siłą rzeczy na programy wpływa rozwój modelu usługowego dotyczącego rozwiązań, które w klasycznej formule opierały się na jednorazowej sprzedaży. Według specjalistów wymusza to zmianę benefitów, szkoleń i modelu rozliczeniowego, ale nawet statusów partnerskich. Marcin Gwara podkreśla, że klasyczny rabat back-end w modelach „commitment" może nie mieć zastosowania, ze względu na stały koszt, który ponosi partner. Podobnie jest ze statusami partnerskimi, które nagradzają partnera dodatkowym rabatem przy każdej transakcji. Przy czym rabat w modelu usługowym może nie mieć zastosowania ze względu na sposób, w jaki dostarczana jest usługa.

– *Chodzi o sytuację, w której partner nie potrzebuje angażować vendora do dostarczenia usługi, przez co nie ma miejsca na zastosowanie takiego rabatu* – wyjaśnia Marcin Gwara.

Ponieważ model as-a-service opiera się na subskrypcjach i cyklicznych opłatach, konieczna jest zmiana struktury prowizji dla partnerów. W wielu przypadkach prowizje mogą być wypłacane w cyklicznych odstępach czasu w oparciu o dalsze utrzymanie klienta.

– *Programy partnerskie w modelu as-a-service zazwyczaj wiążą się z dłuższą relacją z klientem. Oznacza to, że partnerzy muszą nie tylko zdobywać nowych klientów, ale także utrzymywać i dbać o relacje z istniejącymi klientami* – podsumowuje Błażej Kowalkiewicz.

Zdaniem integratora

Piotr Gałecki, prezes, Kreski

Od producentów oczekiwałbym przede wszystkim, aby stosowali się do regulacji ustalonych przez siebie w programach partnerskich. Kolejna kwestia, w której moim zdaniem warto poprawić współpracę na linii vendor – partner, to zaangażowanie Channel Account Managerów. Ostatnio obserwuję, że więcej energii poświęcają na wsparcie klientów końcowych, a nie partnerów. Ponadto nadal brakuje ludzi w zespołach współpracujących z partnerami, a te niedobory i rotacja są chyba nawet większe niż w minionych latach. Istotnym wsparciem w ramach programów partnerskich są natomiast szkolenia. Co miesiąc zatrudniamy nowych pracowników, którzy potrzebują fachowej wiedzy, a ci pracujący dłużej też muszą stale rozwijać kompetencje, więc szkolenia i warsztaty są bardzo potrzebne i jak dla mnie nigdy nie ma ich za wiele, zwłaszcza że wysoko oceniam jakość szkoleń, które są organizowane przez producentów albo dystrybutorów we współpracy z vendorami.

Expert view

Koniec ze skostniałymi programami partnerskimi

„W Fujitsu mówimy: partnerze, chcemy uczyć się od Ciebie. Takie spojrzenie sprawia, że dyskusje są nie tylko ciekawsze, ale również łatwiejsze” – mówi **Marcin Gwara, Channel Manager w Fujitsu.**

■ W jaki sposób dynamiczne zmiany zachodzące na rynku nowych technologii wpływają na kształt programów partnerskich?

Programy partnerskie są na ogół skostniałe i niewiele się od siebie różnią, bazując na tych samych schematach – „przyjdź do nas, weź udział w szkoleniu, a potem dostaniesz dodatkowy rabat na nasze produkty”. To wcale nie jest złe podejście, bowiem wielu partnerom zależy na stabilności i ochronie projektu. Jednak w dynamicznym świecie, w którym żyjemy, zaczyna to nie wystarczać. Dlatego w Fujitsu wychodzimy z założenia, że trzeba dać partnerom odrobinę większą przestrzeń, żeby mogli pokazać siebie i swoją wartość w określonych obszarach. Stąd ważnym elementem programu Fujitsu jest część nazywana ekosystemem. W praktyce oznacza to, że partner opowiada nam o sobie i swoich projektach. W ten sposób zmieniamy narrację. Nie zamierzamy opowiadać wyłącznie o naszym portfolio, lecz chcemy się dowiedzieć, gdzie partner rozwija swój biznes i dopasować się do jego oferty, pokazując szeroką gamę rozwiązań Fujitsu.

■ Jaka jest na to reakcja ze strony partnerów? Czy chcą się dzielić z wami informacjami o swoim biznesie?

Jestem pozytywnie zaskoczony podejściem partnerów. Mam za sobą kilkanaście prelekcji na temat naszego innowacyjnego podejścia do programu partnerskiego. Po każdej wiele osób podchodziło do mnie, pytając jak go realizujemy i jak nawiązać współpracę. Partnerzy często nie zdają sobie do końca sprawy z korzyści, jakie przynosi im praca z vendorem. Z reguły kojarzą Fujitsu ze sprzętem, takim jak serwery czy macierze dyskowe. Jednak po bliższym zapoznaniu się z naszą nową propozycją, otwierają im się oczy. Na przykład kiedy dowiadują się, że możemy rozmawiać o ochronie danych, patrzą na projekt z innej strony i dużo chętniej otwierają się na współpracę. Na początku miałem obawy, że partnerzy nie będą chcieli nam opowiadać o swoim biznesie, dzieląc się własnymi doświadczeniami. Jednak jest absolutnie na odwrót i bardzo się z tego cieszę, ponieważ sukces partnera to sukces producenta.

■ Ale wciąż istnieje liczna grupa partnerów wykazujących znikome zainteresowanie programami partnerskimi. Czy często spotykacie się z taką postawą?

W przypadku tradycyjnych programów partnerskich dostrzegam taką postawę. Partnerzy często pytają, czy trzeba się rejestrować, jakie są z tego benefity, a w 90 proc. przypadków uzyskują odpowiedź, że zdobędą nowe kompetencje, rabaty, status... Partnerzy najczęściej zatem dołączają do programu, aby uzyskać rabat. Jednocześnie są znużeni prośbami vendorów o stworzenie biznes planu czy prowadzenie wspólnych akcji marketingowych. Natomiast w Fujitsu mówimy: partnerze, chcemy uczyć się od Ciebie. Takie świeże spojrzenie sprawia, że dyskusje są nie tylko ciekawsze, ale i łatwiejsze.

■ Na ile partnerów motywują statusy platinum, gold czy silver?

Czasami jest to motywator, bowiem niektórzy klienci wymagają od partnera, aby mógł pochwalić się jakimś statusem, na przykład Expert Fujitsu. W ten sposób można otworzyć wcześniej zamknięte drzwi. Jednak status nie jest aż tak bardzo ważny dla partnera. Przyznawany jest on wyłącznie na rok, a jego uzyskanie wymaga od partnera dużego wkładu pracy. Statusy tracą też na znaczeniu na rynku, gdzie zaczyna dominować sprzedaż konsultatywna i nie wystarczy przesuwanie pudełek z punktu A do punktu B. Zmieniają się wymagania klientów, oczekujących od partnerów wysokiej specjalizacji, a tej nie uzyska się dzięki statusowi u jednego vendora.

■ Nieco inaczej niż konkurenci podchodzicie też do programów lojalnościowych. Na czym polega różnica?

Prowadzimy program lojalnościowy Cyberbonus, który jest początkiem naszego podejścia związanego z budowaniem ekosystemu. Jak każdy inny taki program gratyfikuje on partnerów za sprzedaż produktów, aczkolwiek mogą go tworzyć wspólnie z nami. Przy czym uważnie wsłuchujemy się w ich potrzeby w tym zakresie. Takie podejście zapewnia nam elastyczność, dzięki czemu program lojalnościowy nie jest skostniały, cały czas ewoluując. Oczywiście każdego roku na partnerów czeka specjalna nagroda w postaci wycieczki i są oni zadowoleni z takiej gratyfikacji. Jednakże nie zamierzamy na tym poprzestawać i cała reszta programu lojalnościowego jest tworzona wspólnie z partnerami. To zdecydowanie zachęca integratorów do współpracy z nami.

Program lojalnościowy tworzymy wspólnie z partnerami.

Fot. archiwum

VPP - program dla partnerów Vertiv

Vertiv Partner Program został stworzony, aby umożliwić dystrybutorom i resellerom sprostanie złożonym wymaganiom klientów w zakresie przetwarzania na krawędzi sieci, cyfryzacji i innych przełomowych trendów, które mają wpływ na dzisiejsze centra danych i całą branżę IT. VPP dostępny jest dla partnerów w wybranych krajach Europy i Bliskiego Wschodu, w tym w Polsce.

Regularnie rozwijany portal partnerski gromadzi narzędzia i zasoby potrzebne partnerom do współpracy z zespołem Vertiv:

- **Moduł rejestracji projektów** pozwala uzyskać dodatkowy rabat, wsparcie przedsprzedażowe i ochronę projektu.
- **Szkolenia techniczne i sprzedażowe** umożliwiają zdobycie dodatkowej wiedzy o dostępnych technologiach i rozwiązaniach Vertiv.
- **Centrum marketingowe** z dostępem do materiałów, które można poddać co-brandingowi.
- **Lokalizator partnerów** pozwala dodać profil firmy partnera do strony Vertiv i uzyskać dostęp do leadów sprzedażowych.
- **Narzędzie Vertiv Solution Designer i konfiguratory produktowe** wspierają dobór, konfigurację i ofertowanie.
- **Aplikacje Vertiv XR & Virtual Showroom** ułatwiają prezentację klientom rozwiązań Vertiv, dzięki realistycznym modelom 3D.
- **Dostęp do modułu VIP** – programu motywacyjnego, w którym partner gromadzi punkty za zakupy produktów Vertiv i wymienia je na atrakcyjne nagrody.

Vertiv Partner Program został wzbogacony o system motywacyjny Vertiv Incentive Program (VIP). Zapewnia on partnerom dostęp do sklepu z nagrodami, w którym można wymienić zgromadzone punkty bonusowe na elektronikę, karty upominkowe, czy niepowtarzalne przeżycia.
Partnerzy VIP+ mają również dostęp do ekskluzywnej usługi concierge, która umożliwia dokonywanie zakupów specjalnych nagród niedostępnych w sklepie.

W ramach programu VIP partnerzy mają dostęp do 5 planów promocyjnych, w których punkty bonusowe przyznawane są: na start (bonus do pierwszego zakupu), za sprzedaż codzienną, za sprzedaż wiązaną (gdy partner kupuje rozwiązania z co najmniej 2 kategorii produktowych w kwartale), za częstotliwość zakupów (gdy zakupy rozwiązań Vertiv są dokonywane w więcej niż jednym miesiącu podczas kwartału) oraz za zakupy wyróżnionych produktów.

Poziomy partnerstwa i korzyści

PARTNER SILVER

- Partner Portal
- Szkolenia online, konfiguratory produktów oraz materiały marketingowe
- Vertiv Incentive Program (VIP) – 1–2 proc. zwrotu w formie punktów bonusowych
- Rejestracja projektów
- Lokalizator partnerów

PARTNER GOLD

Dodatkowo:

- Zwiększony zwrot w formie punktów bonusowych (do 2,5 proc.)
- Dostęp do programu demo i możliwość zakupu produktów demonstracyjnych z 50 proc. rabatem

PARTNER PLATINUM

Dodatkowo:

- Dostęp do VIP+
- Zwiększony zwrot w formie punktów bonusowych (do 2,8 proc.)
- Opcjonalny indywidualny plan wzrostu i stały rabat
- Przypisany Account Manager

PARTNER DIAMOND

Dodatkowo:

- Przejście z programu VIP+ na stałe rabatowanie i budżet MDF w oparciu o wspólne plany sprzedażowe i marketingowe oraz indywidualne cele
- Specjalny plan szkoleń

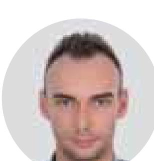
PARTNER DIAMOND ELITE

Dodatkowo:

- Dostęp do i-VIP – to nowa możliwość zdobywania indywidualnych punktów przez pracowników partnera za ich aktywność na portalu i wydawania ich w sklepie z nagrodami
- Indywidualnie ustalony rabat zakupowy

Dołącz do Vertiv Partner Program już dziś, rejestrując się na stronie: Partners.Vertiv.com

Kontakt dla partnerów:
Błażej Kowalkiewicz
Field & Channel Marketing Manager CEE
Blazej.Kowalkiewicz@Vertiv.com



Obserwowalność: nowe, modne słowo?

Nie bez powodu tacy potentaci jak Cisco i Broadcom dokonują wielkich inwestycji, by wykroić sobie jak największy kawałek rynku monitorowania wydajności aplikacji i obserwowalności. Warto zatem bliżej przyjrzeć się temu segmentowi rynku IT.

■ *Tomasz Janoś*

Niedawne, i jak dotąd największe, przejęcie w historii Cisco dotyczyło Splunka, producenta specjalizującego się w monitorowaniu wydajności aplikacji (APM – Application Performance Monitoring) i obserwowalności (Observability). „Razem staniemy się jedną z największych globalnych firm software'owych" – tak komentował transakcję opiewającą na 28 mld dol. Chuck Robbins, dyrektor generalny Cisco. I rzeczywiście koncern, który od lat 80. XX wieku kojarzony był głównie z infrastrukturą sieciową, od dekady coraz bardziej koncentruje się na subskrypcjach oprogramowania i cyklicznych dochodach uzyskiwanych w modelu as-a-service. Akwizycja Splunka ma to jeszcze przyspieszyć. Potentatem na rynku APM & Observability chce być także Broadcom – kolejny producent kojarzony wcześniej przede wszystkim z warstwą sprzętową. Obserwowalność to jeden z celów przyświecających planowanemu zakupowi VMware'a (za bagatela 61 mld dol.) oraz wcześniejszej akwizycji CA Technologies.

Dlaczego potężni inwestorzy tak chętnie wchodzą na ten wyspecjalizowany rynek? Wynika to z tego, że wydajność aplikacji staje się dla użytkowników biznesowych, funkcjonujących w cyfrowym świecie, sprawą kluczową. Problemy z działaniem firmowego software'u mogą mieć zgubny wpływ na lojalność klientów, reputację marki i dochody. I nie jest to już sprawa tego czy – jak dawniej – dział IT miał do sprawdzenia, czy coś działa, czy nie. Jak wynika z badań Akamai zaledwie 1-sekundowe opóźnienie w czasie ładowania strony internetowej skutkuje o 11 proc. mniejszą liczbą jej wyświetleń, o 16 proc. mniejszą satysfakcją klienta i o 7 proc. niższą konwersją osoby przeglądającej daną stronę na aktywnego klienta. Dziś e-commerce nie może sobie pozwolić na takie utrudnienia w biznesie.

> Działy IT coraz częściej **sięgają po APM.**

Podobnie jest w korporacjach, gdzie każdy pracownik potrzebuje wielu różnego rodzaju aplikacji do wykonywania codziennej pracy. Aby zapewnić, że wszystkie procesy przebiegają płynnie, potrzebne staje się ich monitorowanie. W rezultacie, jeśli weźmie się pod uwagę wiele aspektów związanych z wydajnością aplikacji, nie dziwi fakt, że działy IT coraz częściej sięgają po technologię APM, aby zapewnić w trybie ciągłym jak najlepsze doświadczenie cyfrowe swoim użytkownikom.

Ze względu na rosnącą złożoność i szybkie tempo zmian w aplikacjach, rynek APM odnotował znaczny wzrost w ciągu ostatniej dekady i przewiduje się, że trend wzrostowy będzie jeszcze bardziej wyraźny w kolejnych latach. W odpowiedzi na zapotrzebowanie rynku narzędzia APM otrzymują dodatkowe funkcjonalności i ewoluują w kierunku kolejnych obszarów zastosowań.

Przekładając to na liczby, analitycy z Research and Markets oceniają, że globalny rynek APM był w roku ubiegłym warty 7,9 mld dol. Przewidują, że do roku 2030 osiągnie wartość 18,8 mld dol., co daje ➤

Fot. Adobe Stock

średnie roczne tempo wzrostu na poziomie 11,5 proc. w omawianym okresie, a więc od 2022 do 2030 r.

Analitycy IDC podkreślają, że wzrost w obszarze APM jest napędzany potrzebą zarządzania wydajnością aplikacji przez cały cykl ich życia – od DevOps do operacji w środowisku produkcyjnym. Ma to zagwarantować, że doświadczenia użytkownika końcowego będą spełniać coraz bardziej wyśrubowane standardy jakości. Zdaniem analityków satysfakcja użytkownika z wydajności i niezawodności aplikacji ma kluczowe znaczenie dla udanych operacji biznesowych w środowisku cyfrowym.

Czym w ogóle jest APM?

Skrót APM można rozwinąć zarówno jako Application Performance Monitoring, jak i Application Performance Management. Oba pojęcia dotyczą wykrywania i diagnozowania skomplikowanych problemów z wydajnością aplikacji, co ma na celu utrzymanie oczekiwanego poziomu usług. W skrócie sprowadza się to do „przekładania metryk IT na znaczenie biznesowe".

Działanie skutecznego narzędzia APM polega na pomiarze wydajności każdego żądania i każdej odpowiedzi, które składają się na transakcję. Aplikacja może działać wolno z powodu problemu z jedną z jej zależności, takiej jak baza danych, serwer internetowy czy pamięć podręczna. Dlatego ważne jest monitorowanie nie tylko samej aplikacji, ale także wszystkich jej zależności.

APM obejmuje zarówno monitorowanie wydajności aplikacji z technicznego punktu widzenia, jak i wydajności postrzeganej przez samych użytkowników. Ponieważ nowe aplikacje działają na bardzo rozproszonej infrastrukturze, są trudne do monitorowania. Dlatego dobre oprogramowanie APM musi śledzić wszystkie kluczowe części aplikacji, aby ułatwić rozwiązywanie problemów i zarządzanie wydajnością.

Według Gartnera narzędzia do monitorowania wydajności aplikacji powinny spełniać trzy podstawowe kryteria. Po pierwsze, zapewniać monitorowanie front-endowe, które obejmuje stałą ocenę doświadczenia użytkownika oraz monitorowanie transakcji dla użytkowników końcowych – zarówno korzystających z komputerów osobistych, jak i urządzeń mobilnych.

Globalny rynek APM będzie rósł w **dwucyfrowym tempie.**

Po drugie, powinno umożliwiać odkrywanie, śledzenie i diagnostykę aplikacji, co obejmuje wiele funkcji, takich jak automatyczne odkrywanie różnych elementów aplikacji, platformy, frameworki, mikrousługi itp. Dotyczy to też określania relacji między tymi elementami i diagnozowanie ich kodu oraz śledzenie, w jaki sposób aplikacja reaguje na żądania użytkowników.

Po trzecie wreszcie, omawiane narzędzia powinny umożliwiać analizę odnoszącą się do rejestrowania wszystkich danych generowanych przez aplikację, a następnie wykorzystywać różne techniki do odkrywania znaczących wzorców. Pomaga to znaleźć przyczynę problemów wydajności i przewidywać problemy zanim one nastąpią.

Śladami danych

Niedawno Gartner rozszerzył nazwę swojego raportu Magic Quadrant, dotyczącego rynku APM dodając do niej słowo „obserwowalność". Zapewniające tą funkcjonalność narzędzia wykorzystują wspomaganą sztuczną inteligencją analitykę, aby szybko identyfikować lub nawet przewidywać problemy na podstawie zbieranych sygnałów telemetrii. Gartner definiuje ten segment rynku jako „oprogramowanie umożliwiające obserwację i analizę zdrowia aplikacji, ich wydajności oraz doświadczenia użytkownika (UX)". Obserwowalność opiera się na wspomnianej telemetrii, zbieranej z punktów końcowych i usług w wielochmurowym środowisku obliczeniowym. Każdy składnik sprzętowy, oprogramowanie i infrastruktura chmury, a także każdy kontener, narzędzie open-source i mikrousługa generują zapisy wszystkich swoich aktywności w takim złożonym systemie. Trzy rodzaje telemetrii, które są powszechnie używane do opisywania obserwowalności, to logi, metryki i ślady (traces).

Logi stanowią zapis wydarzeń wewnątrz systemu. Z kolei metryki to zestaw wartości, które są monitorowane w czasie. Przykładami metryk mogą być kluczowe wskaźniki wydajności (KPI), wydajność procesora oraz każda inna ocena stanu i wydajności systemu. Ślad jest natomiast efektem śledzenia danego żądania począwszy od interfejsu użytkownika przez cały system i z powrotem, gdy użytkownik otrzymuje potwierdzenie, że jego żądanie zostało zrealizowane. W ramach śladu rejestrowana jest każda operacja wykonana w odpowiedzi na to żądanie.

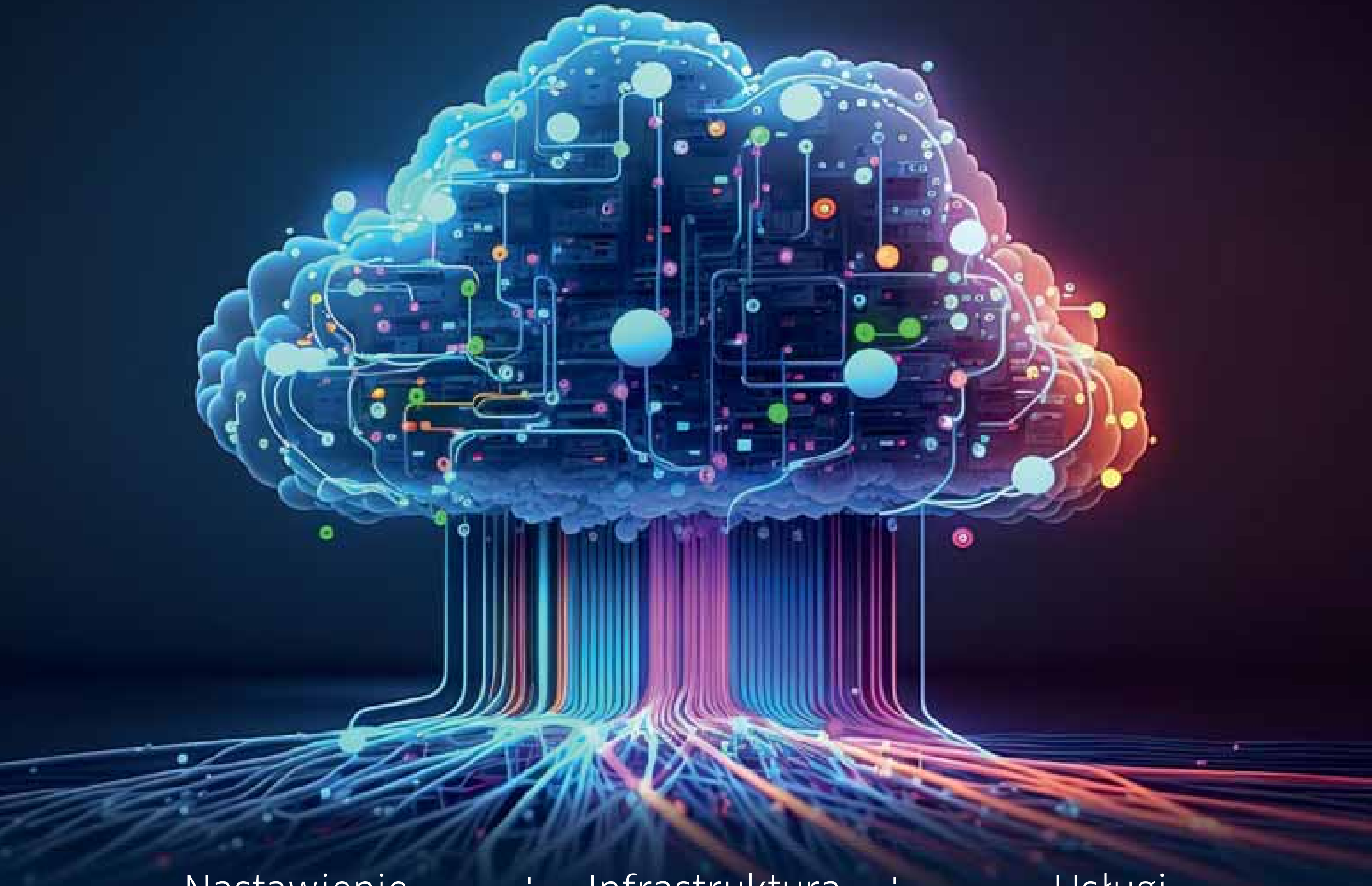
Docelowymi użytkownikami oprogramowania oferującego obserwowalność są działy IT, osoby odpowiadające za działanie serwisów internetowych, specjaliści ds. chmur i platform, programiści aplikacji oraz producenci oprogramowania. ■

OBSERWOWALNOŚĆ to także wyzwania

Wielu dostawców narzędzi z obszaru APM & Observability publikuje co roku raporty o stanie technologii i rynku. Należą do nich Splunk i Observe. Najnowsze badania tego drugiego potwierdzają, że obserwowalność zyskuje na świecie popularność i może być receptą w radzeniu sobie z wyzwaniami, przed którymi stoją nowoczesne firmy. Jednak osiągnięcie obserwowalności wymaga rozwiązania pewnych problemów. Po pierwsze zwiększa się wykorzystanie nowych technologii, takich jak mikrousługi i serverless, a wraz z nimi rośnie złożoność środowisk aplikacyjnych i tym samym poziom trudności w osiągnięciu obserwowalności. Po drugie, chociaż wiele organizacji twierdzi, że stosuje obserwowalność, to wciąż trwa zamieszanie wokół znaczenia tego terminu. Co więcej, niewiele organizacji uważa, że znalazło sposób na mierzenie jej wpływu. Kolejnym problemem jest to, że dane są kluczowe dla osiągnięcia obserwowalności, ale przetwarzanie dużych wolumenów danych może w tym kontekście stanowić wyzwanie. Wedłuch danych Observe wynika, że ponad ¾ badanych organizacji zbiera więcej niż 100 GB danych dziennie, przy czym niemal połowa pozbywa się ich z powodu kosztów przechowywania.

USŁUGI IT DLA PRZEDSIĘBIORSTW

RAPORT



Nastawienie klientów do usług chmurowych: **jak będzie się zmieniać?**

Infrastruktura w modelu usługowym: **czy i kiedy?**

Usługi cyberbezpieczeństwa: **ostatnia deska ratunku?**

Nastawienie do usług *powinno się zmienić*

„Coraz częściej klienci, którzy są na etapie podejmowania decyzji o zaspokojeniu określonej potrzeby biznesowej, najpierw rozważają skorzystanie z usługi chmurowej" – mówi **Mariusz Rzepka, Development Director of MSP & Cybersecurity Services w CEEcloud.**

CRN Już ponad dekadę temu producenci rozwiązań IT przyjęli narrację, że przyszłość rynku należy do usług. Jednak w różnych regionach geograficznych stopień zainteresowania tymi usługami jest bardzo różny, a przedsiębiorstwa z niektórych krajów – w tym z Polski – często wręcz otwarcie wyrażają wobec nich niechęć. Dlaczego?

Mariusz Rzepka To zjawisko można wyjaśnić na kilka sposobów. Głównym jest konserwatywna kultura biznesowa. Niechętnie wdrażamy nowatorskie rozwiązania – wystarczy uświadomić sobie, jak głęboko są u nas zakorzenione takie powiedzenia jak „lepsze jest wrogiem dobrego" albo „jak coś działa, to nie powinno się tego ruszać". Szefowie firm często otwarcie przyznają, że nie potrzebują nic szybszego, skuteczniejszego, wymuszającego zmiany procesów biznesowych itd. Zresztą z kulturą zarządzania wiele wspólnego ma drugie wyjaśnienie tego zjawiska, na które chciałbym zwrócić uwagę. Pracownicy działów IT bardzo obawiają się konsekwencji ewentualnej porażki. Wiedzą, że będą one niewspółmiernie bardziej dotkliwe niż stojąca po drugiej stronie szansa na otrzymanie ewentualnej nagrody lub przynajmniej pochwały za skuteczną realizację projektu, który da firmie realne korzyści. Unikają więc tego ryzyka.

CRN Wyraźnie widać zatem, że mamy tu do czynienia z aspektami psychologicznymi. A czy ewentualnym wyjaśnieniem tej niechęci do usług mogą być kwestie techniczne, takie jak zbyt wolne lub niestabilne łącza internetowe?

Zdecydowanie nie, zresztą w tej kwestii bardzo dużo poprawiło się na skutek pandemii – wyeliminowanie ewentualnych niedoskonałości w infrastrukturze operatorów telekomunikacyjnych wymusili zdalni pracownicy. Obecnie od strony technicznej zupełnie nie odstajemy od innych krajów zachodnich, a często wręcz je wyprzedzamy. Mamy zdywersyfikowany rynek telekomunikacyjny oraz bardzo dobre łącza, także komórkowe.

CRN Na jakie zatem korzyści wskazują te firmy, którym skutecznie udało się wdrożyć model bazujący na szerokim wykorzystaniu usług IT?

Ich argumentacja generalnie jest spójna z tą przedstawianą przez dostawców usług. Wskazują oni na możliwość obniżenia kosztów utrzymania środowiska informatycznego, łatwość wprowadzania zmian, prostą migrację do nowych środowisk, brak konieczności prowadzenia aktualizacji własnych rozwiązań, lepszą kontrolę jakości i przejrzystość ułatwiającą zarządzanie. To wszystko przekłada się na lepsze wykorzystanie budżetów IT, zwiększenie poziomu bezpieczeństwa oraz poprawę jakości pracy w działach IT. Jednak są też korzyści nieoczywiste. Szefowie działów IT w niektórych firmach przyznają, że po wprowadzeniu usług w znacznym stopniu ograniczony został odpływ pracowników z działów IT. Wcześniej narzekali na nerwową atmosferę wynikającą z wysokiego poziomu złożoności zarządzania firmowymi systemami i braku możliwości zagwarantowania ciągłości ich pracy. Wyeliminowana została konieczność natychmiastowego reagowania na problem, wsiadania do samochodu i szybkiej jazdy w miejsce, w którym on wystąpił. Teraz za poradzenie sobie z tym problemem odpowiada usługodawca.

Fot. Adobe Stock

CRN Niektórzy duzi producenci zaawansowanych rozwiązań sprzętowych zadeklarowali jakiś czas temu, że w modelu usługowym, rozliczanym metodą „pay-per-use", chcą mieć dostępne całe swoje portfolio. Czy nie jest na to trochę za wcześnie? Zresztą nie tylko z powodu, póki co, ograniczonego zainteresowania, ale także konieczności pokrycia niemałych kosztów produkcji sprzętu, które zwrócą się nie w momencie sprzedaży, ale zakończenia kontraktu usługowego, a więc po kilku latach. Do tej pory to klient martwił się tym, jak szybko zwróci mu się inwestycja, a teraz – w modelu usługowym – to producent musi się martwić tym, kiedy odzyska te pieniądze...

Dla producentów różnych rozwiązań technicznych finansowanie nigdy nie stanowiło problemu. To są firmy, które mają duże środki finansowe na rozwój produktów w działach R&D czy prowadzenie rozbudowanych działów sprzedaży itd. Wyzwaniem nie jest więc przepływ pieniędzy, ale raczej nakłonienie klienta do zmiany modelu współpracy, swego rodzaju uzależnienie go w postaci długotrwałego kontraktu. Przy czym słowo „uzależnienie" pada tutaj w pozytywnym kontekście. To jest swego rodzaju małżeństwo z rozsądku, z którego obie strony mają czerpać wspomniane już wcześniej korzyści. Praktyka pokazuje, że jeśli dany producent ma bogate portfolio usług, to klient rozpoczynający współpracę w tym modelu i korzystanie z jednej, szybko zacznie interesować się kolejnymi. W tym obszarze dużą rolę do odegrania mają firmy z kanału dystrybucyjnego, które przez lokalizowanie usług, ułatwiają tę współpracę pomiędzy odbiorcą a dostawcą.

CRN No właśnie, gdy popularne stawały się usługi chmurowe, najbardziej przerażoną grupą w kanale sprzedaży rozwiązań IT byli dystrybutorzy, gdyż w tej dziedzinie byli postrzegani jako zbędne ogniwo. Jak kwestia ta wygląda obecnie?

Nasza rola jako dystrybutora w kanale sprzedaży usług praktycznie się nie zmieniła i nadal jest bardzo ważna. Przybliżamy partnerom ofertę dużych usługodawców, szkolimy ich, zapewniamy wielowątkowe wsparcie oraz to, że dana usługa jest świadczona w zgodzie z lokalnym prawem itd. Zniknął jedynie atrybut fizyczności dystrybuowanych rozwiązań. Kiedyś przy każdym wdrożeniu trzeba było dostarczyć sprzęt, skonfigurować go, przeprowadzić testy – to wszystko trwało tygodniami lub dłużej. Wdrażanie usług jest bez porównania szybsze, łatwiej jest też je przetestować, aby zdecydować, czy w ogóle spełnią wymagania klienta. Nic też nie trzeba kupować na zapas, bo zadaniem usługodawcy jest zapewnienie praktycznie nieskończonej skalowalności.

> Usługi to... **małżeństwo z rozsądku,** z którego obie strony mają **czerpać korzyści.**

CRN Czy partnerzy powinni w jakiś specjalny sposób przygotować się do tej transformacji?

Przy przechodzeniu do chmury i usług zarządzanych zewnętrzna firma IT uzupełnia albo wręcz zastępuje działania zespołu IT klienta. Zapewnia aktywne wsparcie w jego biznesie. Ponieważ na rynku dostępnych jest wiele usług zarządzanych, które precyzyjnie określają czego powinien spodziewać się klient, dlatego partner musi przede wszystkim rozumieć jak działa dana usługa, jak jest rozliczana oraz jakie potrzeby klienta adresuje. Drugą, równie ważną rzeczą, jest zdobycie kompetencji przez partnerów. Ich kwalifikacje są kluczowe i powinny być rozwijane, aby uniknąć ryzyka popełnienia błędu w konfiguracji usługi, który mógłby prowadzić do pojawienia się luk bezpieczeństwa lub zbyt wysokich rachunków za usługi. ➤

CRN A jak wygląda podejście partnerów do całkowicie zmienionego modelu rozliczeń?

Dość często partnerzy patrzą na usługi jedynie z perspektywy swoich szybkich zysków. Tymczasem model usługowy, dzięki swojej prostocie i powtarzalności, daje wiele korzyści obu stronom. Ale wymaga świadomych decyzji. Potencjalny partner MSP powinien w strategii swojego rozwoju uwzględniać fakt, że nie będzie otrzymywał jednorazowego zastrzyku finansowego w postaci opłaty za zrealizowane i odebrane przez klienta wdrożenie. W przypadku usług zysk – jeśli już trzymać się terminologii medycznej – spływa jak kroplówka. Bywają sytuacje, że jest to niedogodność, ale praktyka pokazuje, że to korzystne rozwiązanie. Obrotny partner rozszerza grono potencjalnych klientów, których do tej pory nie było stać na drogie inwestycje w IT, dzięki czemu może zagwarantować sobie ciągłość biznesu na kolejne miesiące i lata. Z tej perspektywy zawczasu będzie wiedział na jaki minimalny zysk w tym okresie będzie mógł liczyć. Jako dystrybutor pomagamy partnerom zbudować wewnętrzny system rozliczeń, bo mamy w tym zakresie duże doświadczenie własne oraz wynikające z najlepszych praktyk rekomendowanych przez dostawców usług, które dystrybuujemy. Naszym celem jest stworzenie u każdego partnera efektu marżowej kuli śniegowej, bo dzięki komplementarności wielu różnych usług będą oni mogli zwielokrotnić swoje zyski.

CRN Jakiego typu błędy najczęściej popełniają partnerzy? W jakim zakresie nie są przygotowani do tej transformacji?

Niewiele jest firm, które od razu zaczynają działalność w modelu Managed Service Provider. Z reguły są to integratorzy, którzy są w fazie transformacji swojego modelu biznesowego, ale mają wiele naleciałości z tradycyjnego modelu. Często uważają, że wystarczy wdrożyć rozwiązanie tak jak do tej pory, ale zamiast odebrać jednorazową zapłatę należy rozłożyć ją na wiele rat. Tymczasem w usługach chodzi o coś innego, one muszą być nieustannie rozwijane przez usługodawcę, co oczywiście generuje koszty. Dlatego iloczyn wysokości miesięcznej opłaty abonamentowej oraz ustalonej w kontrakcie liczby miesięcy praktycznie zawsze będzie większy, niż wartość zrealizowanego jednorazowo wdrożenia. Jednak za tym idą korzyści, w tym wspomniana rozbudowa techniczna, o ile zajdzie taka konieczność, a także zawsze zaktualizowane i odpowiednio zabezpieczone oprogramowanie, czy też gwarancja wysokiej dostępności określona w umowie SLA. Do tego trzeba pamiętać, że aby rachunek finansowy się zbilansował, nie można bazować tylko na kilku klientach, ale trzeba ich mieć setki lub więcej – marża ze spływających miesięcznie opłat abonamentowych musi sumarycznie być na tyle duża, aby zagwarantować firmom możliwość nieskrępowanego funkcjonowania. Taka zmiana mentalna nie zawsze jest prosta i często doradzamy nawet dużym integratorom w kwestii tego, jak przejść przez tą transformację.

CRN Jakie usługi cieszą się obecnie największym zainteresowaniem?

Analizując przez pryzmat liczby zapytań, dużym zainteresowaniem cieszą się usługi zarządzania infrastrukturą sieciową, podatnościami, zdalny monitoring i zarządzanie czy archiwizacja poczty elektronicznej. Przy czym liderem – tak samo jak w modelu on-premise – jest oczywiście bezpieczeństwo sieci oraz ochrona hostów przed różnego typu zagrożeniami, w tym głównie przed ransomware i phishingiem. Cieszy mnie też, że – poza wdrożeniem technicznych metod obrony – polscy partnerzy i klienci coraz większą uwagę zwracają na szkolenia pracowników. Od zawsze wiadomo, że w tej kwestii to człowiek jest najsłabszym ogniwem, a temat takich usług jak szkolenia zazwyczaj jest pomijany przez działy IT. Zresztą nie zawsze potrafią one przekazać wiedzę w skuteczny sposób i to jest bardzo duża przestrzeń do działania dla partnerów.

> Oferując usługi trzeba mieć **setki klientów.**

CRN Czy istnieją jakieś obszary, które jeszcze nie zostały zagospodarowane przez partnerów, gdyż nie zdają sobie oni z tego sprawy lub nie są odpowiednio przygotowani?

Największe wyzwanie dotyczy najpopularniejszego tematu, czyli bezpieczeństwa. Chodzi o ochronę dotyczącą bardzo precyzyjnie zdefiniowanych obszarów, jak chociażby wykrywanie ataków man-in-the-middle aktywowanych przez pracowników, który podłączyli do firmowej sieci zainfekowane w innym miejscu urządzenie mobilne. Coraz większym problemem dla firm jest też zjawisko shadow IT. To zazwyczaj z tego powodu dochodzi w firmach do wycieków danych, a zapobiec mogą temu usługi DLP-as-a-Service. Partnerzy powinni zainteresować się także usługami automatyzacji procesów w przedsiębiorstwach, a do realizacji tego celu coraz lepiej sprawdza się sztuczna inteligencja.

CRN Jak reagują klienci na propozycję zmiany modelu nabywania rozwiązań IT z CapEx na OpEx?

Generalnie pozytywnie. Jeszcze dziesięć lat temu klienci chętnie kupowali systemy IT jako inwestycję na trzy lata i często się tym chwalili, bo zwiększały one wartość firmy. Obecnie bywa, że po pół roku użytkowania sprzęt staje się zbyt wolny, przestarzały lub podatny na włamania do infrastruktury klienta, a jego modernizacja kosztowna lub niemożliwa. Należałoby go pilnie wymienić albo przynajmniej utrzymywać pracowników posiadających odpowiednie kwalifikacje, certyfikaty, jak też zapewniać drożejące usługi utrzymania i wsparcia oferowane przez producenta. Z korzystania z rozwiązań w takim modelu ciężko jest się też wycofać, co prowadzi do powstawania długu technologicznego.

CRN Czy firmy doświadczone w obsłudze zaawansowanych środowisk IT w takim modelu są już świadome tych niedogodności?

Oczywiście, wiedzą, że usługi charakteryzują się bardzo niskim kosztem wejścia, a także brakiem ryzyka wystąpienia problemów, gdy konieczne okaże się przeskalowanie takiej usługi. Klienci doceniają obowiązującą w świecie usług zasadę, zgodnie z którą nie trzeba kupować niczego na zapas. Brak takiej możliwości w przeszłości przyczyniał się do marnotrawienia przez firmy bardzo dużych środków, które można było przeznaczyć na stworzenie lepszego produktu dla klientów. Dla firm coraz ważniejsze jest też to, że taki model postępowania jest zgodny ze strategią zrównoważonego rozwoju. Brak konieczności kupowania na zapas powoduje, że trzeba wyprodukować mniej sprzętu, zaś później jest mniej elektrośmieci do utylizacji, co wpływa pozytywnie na środowisko.

CRN Z kim o tego typu zagadnieniach rozmawiać po stronie klienta? Kiedyś zwyczajowo był to dział IT, ale obecnie można spotkać się z rekomendacjami, aby od razu próbować trafić do członków zarządu, na przykład dyrektora finansowego lub wręcz prezesa...

Z mojego doświadczenia wynika, że nie powinno się pomijać działu IT, ale zdecydowanie należy zaczynać od jego szefa, który zresztą w rozwijającej się polskiej kulturze biznesowej coraz częściej jest też członkiem zarządu. To, jeśli będzie taka konieczność, dość łatwo otwiera drogę do innych osób na wysokich stanowiskach, a rekomendacja szefa działu IT może ułatwić asygnowanie odpowiedniego budżetu.

CRN Część potencjalnych klientów, którym oferowane jest skorzystanie z modelu usługowego, wyraża obawę o niekontrolowany wzrost wysokości miesięcznego abonamentu. Jak często zdarza się, że mają rację?

To jest wielowątkowy aspekt. Jeżeli mówimy o usługach, które służą partnerowi jako komponent do stworzenia własnej usługi, to on ponosi ryzyko takiej podwyżki. Zmniejsza się jego marża, co oczywiście może skompensować poprzez restrukturyzację kosztów lub podniesienie abonamentu dla klientów. Natomiast w przypadku, gdy partner tylko odsprzedaje gotową usługę, na przykład w modelu SaaS, to wzrost jej kosztów automatycznie dotyka użytkownika końcowego, ale przy relatywnie łatwej możliwości rezygnacji z usługi jej dostawca ryzykuje odpływem klientów. To duży hamulec dla tego typu działań, a jeśli już dochodzi do podwyżki cen, to usługodawcy zazwyczaj starają się to zrekompensować wzrostem funkcjonalności.

CRN Niemniej rezygnacja z usług chmurowych nie zawsze jest taka prosta. Zdarza się, że ich dostawcy nie umożliwiają masowego eksportu i importu danych użytkowników...

Zgadza się, dlatego zawsze partner i jego klient powinni przeanalizować określone przez usługodawcę warunki wyjścia. Klient musi pamiętać, że finalnie to on ponosi odpowiedzialność za dane. Dotyczy to nie tylko rezygnacji z usługi – dostawca może zakończyć jej świadczenie z różnych powodów. Bywały też przypadki udanych cyberataków, które uniemożliwiały korzystanie z usługi przez dłuższy czas. Dlatego zawsze trzeba zapewnić sobie możliwość backupu danych i odtworzenia ich w innym środowisku. Coraz częściej taką postawę wymuszają też regulacje prawne. Ale w tej kwestii warto podzielić się jeszcze jedną ciekawą obserwacją: nawet jeśli klient rezygnuje z korzystania z danej usługi, to nie chce rezygnować ze wsparcia danego partnera ze względu na zbudowane przez lata relacje i zaufanie.

MARIUSZ RZEPKA
od ponad 20 lat zajmuje się doradztwem i promowaniem nowych technologii oraz usług cyfrowych, w tym cyberbezpieczeństwa. Swoje doświadczenie zawodowe zdobywał na wielu stanowiskach, od menedżera kanału sprzedaży, po dyrektora zarządzającego regionem CEE u takich dostawców jak Fortinet, Sophos, ICsec, czy Cato Networks. W swojej filozofii działania hołduje przekonywaniu zarządów firm do inwestowania zarówno w ludzi, jak i w rozwiązania techniczne, a także do kreowania postaw sprzyjających bezpiecznemu oraz zrównoważonemu rozwojowi biznesu.

CRN To oznacza, że warto mieć w portfolio podobne usługi od konkurencyjnych dostawców...

Tak. Partner, który decyduje się na aktywne oferowanie usług, powinien skompletować ich jak najszersze portfolio – część może pokrywać się funkcjonalnie, co ułatwi ewentualną migrację z jednej usługi do drugiej. Zresztą przeprowadzenie takiej operacji to dla partnera kolejna okazja do zarobku i wykazania się przed klientem.

CRN Czy zdarza się, że klient żałuje rozpoczęcia korzystania z usługi, bo nie zrozumiał jakichś związanych z nią aspektów technicznych bądź finansowych?

Ja nigdy nie miałem do czynienia z taką sytuacją, chociaż jestem świadomy, że pewnie mają one czasem miejsce. Natomiast jeśli do tego dochodzi, to zazwyczaj oznacza, że partner wykonał swoją część pracy w niewystarczający sposób. Zawiodła próba wytłumaczenia, na czym będzie polegała zmiana. Nieporozumienia zazwyczaj zdarzają się w sytuacji, gdy usługa rozliczana jest miesięcznie nie według stałego cennika, ale taryfikatora – wówczas nawet drobny błąd w jej konfiguracji może doprowadzić do znacznego wzrostu miesięcznych rachunków. Jeśli chodzi o funkcjonalność, to tę zawsze bardzo łatwo można sprawdzić – praktycznie każdy usługodawca zapewnia dostęp do wersji demonstracyjnych, dzięki którym można rozwiać wszelkie wątpliwości.

CRN Jak często można spotkać w Polsce firmy, które całościowo przyjęły strategię „cloud first"?

Pomijając relatywnie małe podmioty, raczej trudno jest w tej chwili zbudować swoją działalność biznesową bazując wyłącznie na usługach chmurowych. Warto mieć lokalnie jakiś zasób, chociażby do backupu danych przechowywanych w chmurze. Natomiast coraz częściej można spotkać się z sytuacją, w której klient na etapie podejmowania decyzji o zaspokojeniu jakiejś potrzeby biznesowej za pomocą systemów IT najpierw rozważa skorzystanie z usługi chmurowej. Dopiero wtedy, gdy nie znajdzie satysfakcjonującego go rozwiązania lub nie powiodą się testy, decyduje się na wdrożenie on-premise.

Rozmawiał
Krzysztof Jakubik

Infrastruktura w modelu usługowym: czy i kiedy?

Kolejną rewolucją w branży IT – niemalże na miarę chmury – miała być dostępność zaawansowanych rozwiązań infrastrukturalnych w formie usługi rozliczanej abonamentowo. Oferta ta w niektórych krajach została przyjęta nadspodziewanie dobrze, ale wygląda na to, że w Polsce jeszcze na nią za wcześnie.

Krzysztof Jakubik

Przez ostatnich kilkanaście lat usługi chmury publicznej ugruntowały swoją pozycję na cyfrowym rynku. Obecnie dla klientów oczywiste są zarówno wady, jak też zalety tego modelu dostarczania zasobów oraz płynące z niego czynniki ryzyka. Przez ten czas okazało się ponadto, że chmura nie jest dla każdego – z różnych powodów. W wielu przypadkach przeszkodą bywają regulacje prawne, czasem wprost nakazujące przechowywanie danych lokalnie, a czasem na tyle nieprecyzyjne, że lepiej nie wystawiać się na „strzał" ze strony niekompetentnego w tym obszarze sędziego, gdyby doszło do procesu.

Zdarza się też, że ze względu na charakter przetwarzanych danych niewskazane jest, aby znajdowały się w oddalonym od firmy klienta centrum danych, gdyż ich przesyłanie w tę i z powrotem generuje zbyt duże opóźnienia. Natomiast na pierwszym miejscu rankingu przyczyn wskazywane jest oczywiście ryzyko związane z bezpieczeństwem, chociaż tu ma miejsce dość paradoksalna sytuacja, bowiem dla osób decydujących się z kolei na korzystanie z chmurowych zasobów kluczowym argumentem jest… wysoki poziom bezpieczeństwa i ciągłości pracy.

Jednak utrzymanie klasycznego modelu, zakładającego kupno i wdrożenie we własnej infrastrukturze serwerów oraz pamięci masowych, wiąże się z coraz większą liczbą wyzwań. Jedno z głównych jest związane z nieprzewidywalnym wzrostem ilości danych, w związku ze stale ewoluującymi środowiskami biznesowymi i wprowadzanymi nowymi usługami, co uniemożliwia zaplanowanie skalowalności infrastruktury IT. To prowadzi do sytuacji, w której jedni klienci przeinwestowują, chcąc zapewnić sobie zapasowe zasoby, inni zaś szybko orientują się, że kupili zbyt małe urządzenie i pół biedy, jeśli w miarę bezboleśnie uda się rozszerzyć jego moc obliczeniową lub przestrzeń dyskową. Nierzadko dochodzi wówczas do konieczności przeprowadzenia rozbudowy środowiska w modelu określanym jako forklift upgrade, czyli „wywiezienie wózkiem widłowym" dotychczas stosowanego rozwiązania i zastąpienie go nowym.

Drugi rodzaj wyzwań związany jest z aspektami finansowymi. Rozwiązania IT wciąż uważane są za kosztowne aktywa, zwłaszcza jeśli wymagane jest dokonanie całości płatności za zrealizowane wdrożenie. Rosną też koszty związane z wykupieniem kontraktów serwisowych od producenta oraz zatrudnieniem ekspertów, którzy po stronie klienta będą dbali o utrzymanie sprzętu i zagwarantowanie ciągłości jego pracy (popyt na nich na całym świecie nadal jest znacznie większy niż podaż). Utrudnieniem bywa również konieczność nieustannej edukacji wewnętrznego personelu, ponieważ rozwiązania IT stale ewoluują i trudniej jest nimi zarządzać, aby sprostać wymaganiom biznesowym.

Fot. Adobe Stock

W biurze jak w chmurze

W reakcji na wyzwania, których doświadczają klienci, producenci rozwiązań IT wpadli na prosty i – mogłoby się wydawać – genialny pomysł. Jeżeli jest to konieczne z powodów operacyjnych, niech będą one wdrażane nadal w siedzibie klienta i połączone z jego infrastrukturą, ale rozliczenie będzie następowało nie w modelu projektowym, a subskrypcyjnym. Zadaniem klienta jest zdefiniowanie wymogów technicznych i biznesowych (kryteria dotyczące wysokiej dostępności, ciągłości pracy, czasu przywrócenia środowiska do pracy po awarii itd.), zaś dostawcy usługi – zdefiniowanie parametrów umowy SLA i dotrzymanie ich poprzez wybór odpowiedniego rozwiązania (sprzęt i oprogramowanie), wdrożenie w siedzibie klienta i utrzymywanie w trakcie trwania umowy. Wysokość miesięcznego abonamentu uzależniona będzie od wypożyczonych przez klienta zasobów (pay-per-use).

W tym czasie producent pozostaje właścicielem rozwiązania, ale klient zachowuje kontrolę operacyjną nad zainstalowanymi aplikacjami i danymi. Jeżeli wymagania klienta dotyczące mocy zainstalowanego sprzętu wzrosną, rolą usługodawcy jest jak najszybsza jego rozbudowa – automatycznie też rośnie wysokość miesięcznego rachunku. Natomiast jeśli wymagania klienta zmaleją, możliwe jest działanie odwrotne, czyli przeskalowanie usługi „w dół", ale... nie za darmo. Żeby klient w ogóle mógł skorzystać z takiej opcji, zazwyczaj musi ją wcześniej wykupić. Dostawcy usługi rekompensują sobie w ten właśnie sposób ryzyko biznesowe związane z potencjalnym zmniejszeniem wysokości abonamentu. Jednocześnie przyznają, że sytuacja, w której wymagania klientów maleją, jest praktycznie niespotykana.

Podstawową korzyścią modelu pay-per-use jest wyeliminowanie ryzyka, że posiadane przez klienta rozwiązania staną się przestarzałe po kilku latach – to rolą dostawcy usługi jest dopasowywanie wdrożonych systemów tak, aby spełniały one zdefiniowane oczekiwania techniczne i biznesowe. To ten aspekt sprawia, że wysokość miesięcznego abonamentu jest znacznie większa, niż miałoby to miejsce w przypadku klasycznego leasingu sprzętu.

Jak podkreślają usługodawcy, jest to najczęstszą przyczyną nieporozumień pomiędzy nimi i klientami, przynajmniej na pierwszym etapie negocjacji. Szybkie przemnożenie wartości abonamentu i liczby miesięcy określonych w kontrakcie (najczęściej 60) daje kwotę o kilkadziesiąt procent wyższą. Pomaga dopiero unaocznienie klientowi ukrytych i nieoczywistych kosztów występujących zazwyczaj po jego stronie, które dzięki subskrypcyjnemu modelowi zakupu i wdrażania są eliminowane. Chodzi między innymi o brak konieczności angażowania własnego personelu do obsługi serwisowej sprzętu oraz jego szkoleń. Praktycznie wyeliminowane jest też ryzyko popełnienia błędu przy rozbudowie rozwiązania czy zakłócenia niedostępności danych podczas niepoprawnie przeprowadzonej aktualizacji oprogramowania. Z klienta zdjęta jest również odpowiedzialność za utylizację sprzętu po zakończeniu okresu jego eksploatacji.

Polska specyficznym rynkiem

Swoje produkty w modelu pay-per-use oferuje znakomita większość producentów zaawansowanych rozwiązań IT. Dominują dostawcy macierzy dyskowych, bowiem pamięci masowe to ta grupa produktów, które relatywnie najłatwiej jest rozbudować pod kątem przestrzeni dyskowej, ale jednocześnie wyzwaniem jest zapewnienie wydajności odpowiadającej zapotrzebowaniu aplikacji. Ich użytkownicy zazwyczaj mają z tym problem, bowiem do stworzenia skalowalnego w odpowiednim stopniu środowiska potrzeba jest doświadczenia, a tym mogą pochwalić się głównie producenci rozwiązań i ich partnerzy.

Kluczowe jest zaangażowanie ze strony partnerów.

Kolejną grupą produktów, która w ramach usług pay-per-use reprezentowana jest najczęściej, są serwery. Oferta tych bywa jednak ograniczona do modeli wykorzystywanych w środowiskach wirtualizacji oraz przetwarzania wysokiej wydajności (high performance computing), bowiem to najczęściej w nich dochodzi do potrzeby zapewnienia skalowalności na trudną do oszacowania skalę. W ograniczonym jak na razie zakresie w modelu usługowym oferowana jest infrastruktura sieciowa oraz stacje robocze.

Systemy oferowane w modelu pay-per-use przeznaczone są do wdrażania w siedzibie firmy klienta, ale zazwyczaj ich producenci deklarują, że mogą być zainstalowane także w obiekcie świadczącym usługi kolokacyjne. Aby proces udostępniania dodatkowej mocy obliczeniowej, pamięci czy przestrzeni dyskowej został uruchomiony jak najszybciej, dostawcy usług pay-per-use zazwyczaj wdrażają o 20–30 proc. więcej zasobów niż zadeklarowane w zamówieniu. Klienci zaczynają za nie płacić w modelu abonamentowym dopiero wtedy, gdy zaczynają z nich korzystać.

Oferta usług pay-per-use dostępnych w portfolio poszczególnych dostawców jest jednak ograniczona geograficznie. W Polsce można nabyć rozwiązania trzech, będących liderami, jeśli chodzi o zakres oferty: Dell, Fujitsu i HPE. Wszystkie te firmy współpracują z partnerami kanałowymi, chociaż prowadzą też bezpośrednią sprzedaż tych usług. Przykładowo, partnerzy oferujący usługi pay-per-use pod marką APEX mogą współpracować z ich dostawcą – Dell Technologies – na kilka sposobów.

– *Są wynagradzani nawet jeśli ich rola przy odsprzedaży usługi ograniczała się do wygenerowania leada poprzez zarejestrowanie go w systemie partnerskim Dell lub dystrybutora. Jeśli partner ma odpowiednie kompetencje i status, może dostarczyć usługi wdrożenia sprzętu albo być dodatkowo hostem usługi, w ramach której udostępni przestrzeń serwerowni do kolokacji sprzętu. W zależności od wybranej przez klienta opcji partnerzy dodatkowo mogą zarządzać sprzętem, a także zaoferować usługi APEX pod własną marką, rozdzielając wdrożoną we własnej siedzibie infrastrukturę między swoich klientów* – podkreśla Michał Gazda, Senior Account Executive w polskim oddziale Della.

Co zaś z producentami, którzy nie wprowadzili do Polski oferty usługowej, mimo posiadania lokalnego przedstawicielstwa? Oficjalnie nie wypowiadają się na ten temat, ale w nieoficjalnych rozmowach przyznają, że polski klient jest dość specyficzny, a przy podejmowaniu decyzji kluczowym kryterium pozostaje wrażliwość na cenę. Porównanie uiszczanej jednorazowo ceny za zrealizowane wdrożenie z łączną wartością wniesionych w modelu usługowym opłat abonamentowych wychodzi mocno na niekorzyść tych drugich. W tej sytuacji

Porównanie modeli wdrażania rozwiązań infrastruktury IT

Kryterium	Tradycyjne wdrożenie	Model pay-per-use	Chmura publiczna
Forma nabycia rozwiązania	Klient kupuje rozwiązanie i opłaca je w całości lub korzysta z leasingu (wydatki kapitałowe – CapEx).	Klient wynajmuje rozwiązanie wyposażone w zasoby o ilości wynikającej ze zdefiniowanych potrzeb biznesowych i technicznych, rozliczenie następuje na bazie miesięcznego abonamentu według cennika (koszty operacyjne – OpEx).	Klient wynajmuje zasoby infrastruktury IT w modelu usługowym (Infrastructure-as-a-Service) i płaci za nie w modelu abonamentowym, według aktualnego zużycia.
Miejsce wdrożenia	Siedziba firmy lub kolokacyjne centrum danych.	Siedziba firmy lub kolokacyjne centrum danych.	Centrum danych dostawcy usług chmurowych.
Skalowalność	Ograniczona, uzależniona od możliwości technicznych danego rozwiązania.	Ograniczona, uzależniona od możliwości technicznych danego rozwiązania, ale w gestii dostawcy usługi jest, aby zapewnić dodatkowe zasoby lub nowe rozwiązanie na życzenie klienta.	Praktycznie nieograniczona dzięki wirtualizacji udostępnianych zasobów.
Odpowiedzialność za serwisowanie	Obsługa przez własny, kosztowny w wykształceniu i utrzymaniu personel. Alternatywnie możliwość skorzystania z usług partnera.	Klient zachowuje kontrolę operacyjną nad aplikacjami i danymi, ale to usługodawca odpowiada za serwisowanie wynajmowanego rozwiązania oraz wsparcie techniczne (część prac wykonuje zdalnie, ale bywa konieczna wizyta w siedzibie klienta).	Operator usługi ponosi pełną odpowiedzialność za rozwiązanie i eliminowanie wszystkich problemów oraz czynników ryzyka.
Cykl życia rozwiązania	Wymagania dot. konfiguracji z czasem stają się nieaktualne, co prowadzi do konieczności – jeśli to możliwe – rozbudowy lub wymiany rozwiązania na nowe.	Zadaniem dostawcy usługi jest zapewnienie, aby spełnione zostały wymagania klienta. W związku z tym bywa konieczna znaczna rozbudowa rozwiązania lub jego wymiana na nowe, z zapewnieniem migracji danych i ciągłości usług.	Usługodawca gwarantuje stały dostęp do usług przez czas trwania kontraktu, więc pojęcie zarządzania cyklem życia rozwiązania z perspektywy klienta nie istnieje.
Efektywność finansowa	Ze względu na możliwe utrudnienia w rozbudowie rozwiązania, zakupy często dokonywane są na zapas, a zasoby, których wartość spada, nie są wykorzystywane przez długi czas.	Klient płaci za wykorzystywane zasoby zamówione w ramach usługi i ma możliwość ich rozbudowy wraz z proporcjonalnym wzrostem abonamentu, ale rezygnacja z części zasobów w celu zmniejszenia wysokości abonamentu zazwyczaj wiąże się z dodatkowymi opłatami.	Klient zachowuje pełną elastyczność finansową, jeśli chodzi o stopień wykorzystania zasobów infrastruktury IT.

w sprzedaży usług nie pomaga tłumaczenie o ich dodatkowych zaletach, tym bardziej, że często dotyczą one aspektów związanych z personelem IT (ten w Polsce nadal jest tańszy „w obsłudze" niż na Zachodzie) albo gwarancji zapewnienia ciągłości biznesowej, do której wciąż często podchodzimy w nonszalancki sposób. W efekcie jako modelowego klienta na rozwiązania IT dostępne w modelu usługowym można w tej części Europy wskazać jedynie duże firmy, dla których dwie wymienione kwestie mają duże znaczenie.

Pay-per-use nie tylko w DC

Metoda pay-per-use nie jest oczywiście nowym wynalazkiem – już ponad 10 lat temu w Polsce pojawiały się firmy oferujące w tym modelu komputery PC, a następnie drukarki. Zainteresowanie wynajmem tych pierwszych jest umiarkowane, ale rozliczanie kosztów druku za każdą stronę w końcu się na rynku przyjęło. Być może dlatego, że w proces ten zaangażowani zostali partnerzy, którzy mają znacznie lepsze dotarcie do potencjalnego klienta, niż producenci.

Zaangażowanie partnerów jest ważne o tyle, że w przypadku zaawansowanych usług często świadczone są one przez producentów bezpośrednio z globalnej lub regionalnej centrali, a więc nie po polsku. W przypadku dużych odbiorców nie powinno stanowić to problemu, ale wśród mniejszych klientów już tak – być może jest to jedno z kryterium, dlaczego są oni rzadziej zainteresowani usługami. Poza tym partnerzy dzięki usługom zyskują szanse na wykazanie się kreatywnością.

– Rozwijamy nasze rozwiązania, a także usługi Security Operations Center, Managed Detection and Response oraz Incident Response w taki sposób, aby mogły być zarówno odsprzedawane przez partnerów, jak też wykorzystywane przez nich do budowy własnych usług. W tym pierwszym przypadku partner otrzymuje prowizję, a jeśli taka będzie wola klienta, to może uzyskać też dostęp do portalu wsparcia i mieć stały wgląd w proces rozwiązywania danego problemu albo wręcz móc inicjować reagowanie na zagrożenia – mówi Robert Dąbrowski, CISSP Manager Systems Engineering w polskim oddziale Fortinetu.

Możliwe do uzyskania korzyści z modelu usługowego są nie do przecenienia i z pewnością nie można ignorować tego zjawiska na rynku IT. Usprawiedliwione wydaje się porównanie jego obecnego etapu dojrzałości do pierwszych lat funkcjonowania chmury. Z pewnością ten rodzaj biznesu nie jest optymalny dla każdego partnera, jak też występuje wiele ograniczeń po stronie klientów. Jednak zainteresowanie się tym modelem odpowiednio wcześnie ułatwi wykrojenie przyzwoitego kawałka tortu, gdy stanie się on bardziej popularny. ■

Trzy pytania do...

Artura Kamińskiego,
Chief Technologist w Apex.it

Dotychczas polscy użytkownicy wykazują relatywnie niewielkie zainteresowanie usługami IT świadczonymi w modelu pay-per-use. Nie oferują ich również wszyscy producenci, którzy mają te usługi w portfolio w krajach zachodnich. Dlaczego?

Popularność tego typu usług stale rośnie, ale rzeczywiście uzyskanie efektu skali jeszcze jest przed nami. Jedną z przyczyn dotychczasowego ograniczonego zainteresowania jest stosunkowo prosta dostępność funduszy krajowych i unijnych, pozwalających na finansowanie infrastruktury IT, które – z racji tego, że przyznawane są w postaci grantu – wymuszają konieczność jednorazowej opłaty za zrealizowane wdrożenie. W wielu krajach z usług pay-per-use mogą też korzystać instytucje publiczne, podczas gdy w Polsce jest to wciąż mocno ograniczone. Niewiele podmiotów publicznych chce wejść w rolę pioniera i procesować pozyskanie infrastruktury w modelu innym od tradycyjnego, jednorazowego zakupu. Wierzę jednak, że to się zmieni, gdyż model usługowy jest bardzo opłacalny w przypadku środowisk IT, które stale rosną, ale w niejednolitym tempie.

Jacy klienci są najczęściej zainteresowani usługami pay-per-use i na które produkty oferowane w tym modelu najczęściej się decydują?

Raczej trudno jest dokonać takiej klasyfikacji poprzez pryzmat wielkości firmy lub charakteru jej działalności. Tak jak wspomniałem, największą korzyścią w przypadku modelu usługowego jest brak konieczności kupowania na zapas, więc siłą rzeczy sprawdzi się on w podmiotach o trudnej do oszacowania skali wzrostu. Należy też zakładać, że z ekonomicznego punktu widzenia na razie w modelu usługowym opłaca się realizować większe projekty. Takie, w których narzut usługodawcy, związany z zapłatą za konieczność administrowania takimi rozwiązaniami, zostanie zniwelowany innymi korzyściami płynącymi z usługi. Sytuacja ta powoduje, że klienci w modelu usługowym najczęściej kupują pamięci masowe i serwery, ponieważ to właśnie w kwestii przestrzeni dyskowej i mocy obliczeniowej najtrudniej jest oszacować wzrost zapotrzebowania w przyszłości, gdy firma będzie realizowała nowe projekty lub rozbudowywała istniejące. Dodatkową korzyścią jest dostęp do ujednoliconej platformy umożliwiającej zintegrowane zarządzanie całym środowiskiem, w tym serwerami i pamięciami masowymi.

Jako firma integratorska macie status partnera HPE uprawniający do pośredniczenia w oferowaniu usług HPE GreenLake. Na czym konkretnie polega wasza rola?

W aspekcie technicznym w dużej mierze jest ona podobna do tradycyjnych wdrożeń – instalujemy dostarczany klientowi sprzęt, konfigurujemy, ewentualnie dokonujemy migracji danych, a w trakcie trwania usługi prowadzimy część prac serwisowych. Największa zmiana ma miejsce przed podpisaniem umowy, bowiem musimy bardzo precyzyjnie rozpoznać potrzeby klienta i charakter jego działalności, przedstawić mu zasady, na jakich oferowane są usługi i upewnić się, że pasują one do jego modelu biznesowego. Klient chce pozbyć się odpowiedzialności za funkcjonowanie danego fragmentu infrastruktury, więc tę na siebie bierzemy my, w zamian za marżę, która jest wliczona w część opłaty za usługę. W Polsce ogniwem pośredniczącym jest też dystrybutor, którego zadaniem jest dbałość o aspekty zgodności z prawem, a także kwestie finansowania.

Usługi cyberbezpieczeństwa: ostatnia deska ratunku

Fot. Adobe Stock

Nakłady ponoszone przez firmy na systemy bezpieczeństwa IT są niewspółmierne do osiąganych rezultatów. Jedną z przyczyn jest deficyt specjalistów, a remedium mogą stanowić usługi.

■ *Wojciech Urbanek*

Systemy edukacji skupiają się na kształceniu prawników, marketingowców czy księgowych. Dlatego firmy nie mają większych trudności ze znalezieniem fachowca w jednej z tych profesji. Zupełnie inaczej wygląda sytuacja w przypadku specjalistów ds. cyberbezpieczeństwa. Jeszcze dekadę temu mało który z pracodawców myślał o etacie dla osoby zajmującej się ochroną zasobów informatycznych. Tym samym placówki edukacyjne na całym świecie nie nastawiały się na kształcenie specjalistów w tej dziedzinie, „produkując" magistrów od zarządzania i marketingu.

Nasilająca się fala cyberataków, a także nowa generacja narzędzi przeznaczonych do ochrony sieci i urządzeń końcowych, sprawiły, że właściciele firm zaczęli coraz bardziej nerwowo rozglądać się za ludźmi, którzy znają się na rzeczy. Popyt na tę grupę pracowników zaczął wyraźnie przewyższać podaż. Według szacunków HRK ICT na polskim rynku jest ponad 17 tysięcy nieobsadzonych stanowisk specjalistów ds. bezpieczeństwa IT. Co gorsza, rekruterzy nie mają nadziei na poprawę sytuacji. Wręcz przeciwnie, pojawiają się opinie, że liczba wakatów z roku na rok będzie się powiększać. Prawdopodobnie część firm będzie zatem zmuszona poszukać alternatywy dla fachowca na etacie. Szczególnie dotyczy to małych i średnich firm, których zazwyczaj nie stać na zaspokojenie wymagań finansowych specjalistów ds. bezpieczeństwa. Według „Ogólnopolskiego Badania Wynagrodzeń" mediana zarobków w tej grupie zawodowej wynosi 9,4 tys. zł brutto.

> Na polskim rynku **brakuje kilkunastu tysięcy** specjalistów.

Producenci nie pomagają

Teoretycznie przedsiębiorcy mogliby wiązać nadzieje ze sztuczną inteligencją, której tak bardzo obawiają się przedstawiciele wielu zawodów. Jednak wiele wskazuje na to, że spece od cyberbezpieczeństwa mogą nie tylko spać spokojnie, ale wręcz przebierać w ofertach pracy jak w ulęgałkach. Po części jest to zasługa dostawców systemów bezpieczeństwa, którzy kilka lat temu ruszyli firmom na pomoc z takimi narzędziami jak EDR (Endpoint Detection and Response), NDR (Network Detection and Response), a od niedawna również XDR (Extended Detection and Response). „Drogi kliencie, powiadomimy Cię, kiedy wydarzy się coś złego, niemniej ktoś u Ciebie w firmie musi sprawdzać i analizować alerty" – to nowe przesłanie producentów. Niektórym przedsiębiorcom udaje się znaleźć takich specjalistów. Z kolei innym jedynie wydaje się, że takowych posiadają i po roku, a czasami później, okazuje się, że obsługa EDR-a bądź XDR-a przerasta możliwości zatrudnionych pracowników. Jednak nie można powiedzieć, że obecni dostawcy EDR, XDR czy SIEM nie wykonują dobrej roboty. Specjaliści przyznają, że po prostu podejście uniwersalne w zakresie bezpieczeństwa też ma swoje ograniczenia.

Złożoność narzędzi, a co za tym idzie trudności związane z interpretacją wysyłanych przez nie sygnałów, to nie jedyny problem, z jakim borykają się menedżerowie wyższego szczebla bądź właściciele firm. Osobnym wyzwaniem pozostaje liczba rozwiązań bezpieczeństwa IT, jakie są stosowane w poszczególnych firmach. Z badania Panaseer 2022 Security Leaders Peer Report wynika, że przeciętna korporacja korzysta z… 70 narzędzi bezpieczeństwa. W przypadku małych i średnich przedsiębiorstw może być jeszcze gorzej, ponieważ bezpieczeństwo IT staje się coraz bardziej złożone w związku z rosnącym wykorzystaniem usług chmurowych i liczbą używanych aplikacji SaaS (średnio firma korzysta ze 130 takich programów). To wymaga od pracowników wyższego poziomu wiedzy technicznej.

Niestety, liczba używanych narzędzi nie idzie w parze z jakością. Zwiększenie wy-

datków na bezpieczeństwo nie ograniczyło liczby cyberataków, a zwłaszcza szkód finansowych, które są przez nie wywoływane. Według analityków Gartnera w 2015 r. wartość globalnego rynku bezpieczeństwa wynosiła 75 mld dol., a na koniec bieżącego roku ma to być już 188 mld. Natomiast specjaliści Cybersecurity Ventures wyliczają, że straty gospodarki światowej z tytułu cyberataków wyniosą 8 bilionów dol. Jeszcze gorzej przedstawiają się prognozy analityków tej firmy. Otóż ich zdaniem w najbliższych latach ta niechlubna wartość ma rosnąć w tempie 15 proc. rocznie, by w 2025 r. osiągnąć poziom 10,5 bilionów dol. Dla porównania, w 2015 r. globalne szkody spowodowane przez cyberprzestępców miały sięgnąć 3 bilionów dol.

Przedstawiciele branży cyberbezpieczeństwa podkreślają, że płynący na konta przestępców strumień pieniędzy byłby jeszcze większy, gdyby nie duże inwestycje w systemy bezpieczeństwa IT poczynione przez użytkowników biznesowych. Jednak wciąż nam daleko do stanu, kiedy liczba incydentów cybernetycznych będzie odwrotnie proporcjonalna do podejmowanych przez firmy wysiłków i wydatków w zakresie działań defensywnych.

Cyberbezpieczeństwo jako usługa

W obecnych czasach ciężko znaleźć firmę, która zatrudnia na etatach pracowników do ochrony mienia. Niemal wszyscy korzystają z usług firm zewnętrznych. Niewykluczone, że w tym samym kierunku będzie podążać rynek usług cyberbezpieczeństwa. Z tą różnicą, że zupełnie innych umiejętności wymaga się od pracowników chroniących zbiorniki z paliwem, fabryczne maszyny czy kontenery z żywnością, aniżeli osób odpowiadających za bezpieczeństwo zasobów IT. Tych ostatnich jest na rynku pracy zdecydowanie mniej, a więc zgodnie z zasadami ekonomii usługi cyberbezpieczeństwa powinny być droższe niż usługi ochrony obiektów przemysłowych.

Według Gartnera w ubiegłym roku wydatki na usługi bezpieczeństwa, takie jak doradztwo, wsparcie sprzętowe, usługi wdrożeniowe i outsourcing, wyniosły 72 mld dol., zaś w roku bieżącym ma to być 76,5 mld. Globalnie dużą popularnością cieszą się usługi MSSP (Managed Security Service Providers). Jak wynika z danych Allied Market Research wartość tego segmentu rynku w 2020 r. wyniosła 22,45 mld dol., a prognozy mówią o 77,1 mld w roku 2030. To oznacza tempo wzrostu na poziomie niemal 13 proc. rocznie. Najbardziej lukratywną grupę dla dostawców MSSP stanowią banki oraz instytucje finansowe, których wydatki na ten cel stanowią około 40 proc. całego rynku. Natomiast najszybciej w latach 2020–2030 ma rosnąć grupa klientów z branży produkcyjnej.

> Zwiększenie wydatków na bezpieczeństwo nie ograniczyło **liczby cyberataków.**

Jakby jednak nie patrzeć na powyższe dane, to pokazują one nieco zafałszowany obraz rynku. Po pierwsze banki czy duzi ubezpieczyciele bardzo często korzystają z usług globalnych koncernów konsultingowych, a wartość podpisywanych kontraktów nijak ma się do segmentu małych i średnich przedsiębiorstw (MŚP). Wiele wskazuje na to, że to właśnie nie największe firmy będą podpisywać najwięcej kontraktów z dostawcami MSSP. Niewykluczone, że początkowo podejmą próby poszukiwania i zatrudniania specjalistów ds. bezpieczeństwa, niemniej w dłuższej perspektywie czasu dadzą o sobie znać ograniczenia budżetowe, a także deficyt odpowiednich fachowców na rynku pracy.

Po drugie, zdecydowanym prymusem na rynku MSSP są Stany Zjednoczone, które ze względu na sposób prowadzenia biznesu różnią się do państw europejskich. Na przykład w USA działa wielu dostawców (w tym Soteria, Recon InfoSec, TrustedSec, Binary Defense), którzy zajmują się technicz- ➤

nym doradztwem w zakresie cyberbezpieczeństwa. Wymienione firmy zatrudniają wysokiej klasy inżynierów, architektów systemów bezpieczeństwa IT, zapewniając swoim klientom kompleksową obsługę w tym zakresie. Innym ciekawym zjawiskiem występującym za oceanem są przejęcia na rynku MSSP. Mniejsi dostawcy usług są połykani przez dużych graczy, chcących w ten sposób umocnić swoją pozycję liderów, rozszerzyć działalności, a także pozyskać najlepszych specjalistów z rynku pracy. Portal MSSP Alerts donosi, że w 2022 r. zarejestrowano aż 50 takich transakcji, co niewątpliwie świadczy o żywotności tego segmentu w Stanach Zjednoczonych.

– Amerykanie są bardziej otwarci na rozmowy niż Europejczycy. Wykazują większe zainteresowanie niż Polacy usługami chmurowymi, a jednocześnie są przy tym bardzo wymagający. Tym, co wyróżnia USA na tle Niemiec czy Polski, jest bardzo duża popularność usług zarządzanych oferowanych przez Managed Service Providerów. Za oceanem rośnie liczba przedsiębiorców, którzy wolą skorzystać z oferty wyspecjalizowanych firm zewnętrznych niż szukać pracowników na etat – mówi Michał Wendrowski, CEO Rublonu, polskiego dostawcy systemów MFA, który działa w USA od kilku lat.

Zdaniem integratora

Daniel Kamiński, Senior Solution Architect, Orange

Do rosnącej popularności usług cyberbezpieczeństwa przyczynia się skala i rodzaj ataków hakerskich. Prawdziwą plagą są wiadomości phishingowe, w których przestępcy podszywają się pod dostawców usług kurierskich, bankowych czy energetycznych. Potwierdzają to choćby dane z raportu CERT Orange Polska za ubiegły rok. Phishing stanowi ponad 42 proc. wszystkich zagrożeń. Kolejne miejsca należą do ataków DDoS oraz złośliwego oprogramowania typu malware czy ransomware. To powoduje, że coraz więcej firm i instytucji myśli o poprawie zabezpieczeń swoich systemów, ale też edukacji dotyczącej internetowego bezpieczeństwa swoich pracowników. Nic więc dziwnego w tym, że rynek usług cyberbezpieczeństwa cały czas się rozwija, a przy tym jest mocno rozproszony. To rozdrobnienie pozwala poświęcić uwagę wielu różnym aspektom z dziedziny cyberbezpieczeństwa i wspierać rozwój także niszowych rozwiązań. My promujemy kompleksową ochronę przed internetowymi zagrożeniami. W tym celu korzystamy ze specjalistycznych rozwiązań mniejszych firm. To pozwala na szybszą reakcję na zmiany trendów. Zakładam, że pewna stabilizacja nastąpi po wdrożeniu wymagań wynikających z nowych dyrektyw, przede wszystkim NIS2 czy DORA.

Leszek Tasiemski, wiceprezes ds. zarządzania produktami, WithSecure

Do popularyzacji usług cyberbezpieczeństwa na polskim rynku przyczynia się rosnąca świadomość zarządów firm na temat zagrożeń. Decydenci zrozumieli, że utrzymywanie własnych zespołów specjalistów ds. cyberbezpieczeństwa jest bardzo kosztowne. Co więcej, zewnętrzni dostawcy mają dużo szerszy obraz występujących incydentów. Tym samym można oczekiwać większej skuteczności w monitorowaniu i wykrywaniu zagrożeń oraz reagowaniu na nie. Istotne są również rozmaite regulacje, które nakładają na firmy obowiązki w zakresie ochrony danych. Firmy, które wcześniej mogły ignorować kwestie cyberbezpieczeństwa, teraz nie mają takiej możliwości.

Polski kierunek

Nad Wisłą rynek usług cyberbezpieczeństwa dopiero raczkuje. W związku z tym dostawcy rozwiązań bezpieczeństwa IT, a także sami integratorzy, muszą wybrać odpowiednią strategię. Coraz częściej słychać zachętę, aby integratorzy wprowadzili do swoich ofert EDR lub XDR w modelu usługowym.

– Spodziewamy się, że coraz większą popularnością będą się cieszyć usługi bazujące na Exposure Management, w przypadku których nacisk kładziony jest na przewidywanie incydentów i zapobieganie im poprzez ciągłe monitorowanie i ograniczanie powierzchni ataku – zauważa Leszek Tasiemski, wiceprezes WithSecure.

> Wzrośnie popularność usług bazujących na **Exposure Management.**

Zmiana podejścia wymaga zwiększonego nacisku na edukację partnerów. Jednym z producentów, który stawia restrykcyjne wymagania wobec partnerów zainteresowanych sprzedażą usług cyberbezpieczeństwa, jest Cisco. W tym przypadku kandydaci muszą przejść przez ścieżkę edukacyjną obejmująca produkty, które chcą wykorzystać w swojej ofercie usługowej. Przedstawiciele Cisco tłumaczą swoją politykę obawami, że firma pozbawiona odpowiedniej wiedzy może skompromitować nie tylko siebie, ale również własne produkty czy technologię. Zresztą historia zna już przypadki, kiedy dostawcy MSSP sami padali ofiarą ataków ransomware.

Nie mniej poważnie podchodzą do tematu usług cyberbezpieczeństwa dystrybutorzy. Przy czym przykładowo Dagma posiada w ofercie zarówno gotowe rozwiązania dla żółtodziobów, jak i takie dla partnerów bardzo dobrze zaznajomionych z tematyką, którzy chcą wnieść do nich swoją wartość dodaną. Z kolei Bakotech we własnym zakresie hostuje usługi adresowane dla MŚP lub zleca to zadanie vendorowi. W rezultacie dystrybutor lub producent odpowiadają za parametry usługi, zaś na barkach integratora spoczywa obowiązek zabezpieczenia infrastruktury.

Popularyzacja usług cyberbezpieczeństwa w Polsce zależy od postawy integratorów oraz klientów końcowych. Ci pierwsi muszą zacząć myśleć po nowemu i przestawić się ze sprzedawcy antywirusów i firewalli na dostawcę usług. Wbrew pozorom nie jest to wcale łatwe zadanie (więcej na ten temat w rozmowie z Mariuszem Rzepką z CEEcloud, pt. „Nastawienie do usług powinno się zmienić”, str. 36). Zdecydowanie łatwiej będzie o zmianę nastawienia wśród małych i średnich firm. Przedsiębiorcy z tego sektora, rozczarowani niemożnością zadbania w własnym zakresie o bezpieczeństwo IT, znacznie ograniczą zakupy „magicznych pudełek” i sięgną po pomoc specjalistów z zewnątrz. ■

Platforma cyberbezpieczeństwa dla dostawców usług

Acronis umożliwia partnerom MSP świadczenie zaawansowanych usług, których celem jest ochrona zasobów IT. Mogą zapewnić swoim klientom backup rozszerzony o przywracanie pracy po wystąpieniu awarii, zabezpieczenie EDR, likwidację źródeł wycieku wrażliwych danych i zarządzanie maszynami.

Truizmem stało się stwierdzenie, że cyfrowe bezpieczeństwo staje się dla wielu firm coraz większym wyzwaniem. Ze względu na swoją złożoność, wielowymiarowość oraz koszty związane z utrzymaniem kompetentnego personelu i wielu narzędzi, przedsiębiorstwa każdej wielkości coraz częściej skłaniają się ku usługom Security as a Service. Umożliwiają one odciążenie personelu IT, ale również pozwalają na wykorzystanie doświadczenia, umiejętności i szerokiej gamy narzędzi, jakimi dysponują usługodawcy zajmujący się takimi zagadnieniami.

Z myślą o tym specjaliści Acronisa stworzyli dla dostawców usług zarządzanych (Managed Service Providers) platformę **Cyber Protect Cloud**, która umożliwia im zaadresowanie wielu potrzeb klientów bez konieczności angażowania znacznej liczby odrębnych/niezależnych narzędzi. Wyróżnia się ona połączeniem szeregu funkcji pomagających zabezpieczyć dane przedsiębiorstwa oraz zapewniających szybkie i sprawnie przeprowadzenie działań naprawczych w przypadku wystąpienia incydentu. Oprócz backupu i klasycznej ochrony antywirusowej, antyspamowej i antyphishingowej, możliwe jest także zabezpieczanie platform komunikacyjnych Microsoft 365 oraz Google Workspace, a także danych z takich aplikacji, jak OneDrive, Sharepoint i Teams.

Bezpieczeństwo to nie tylko backup

Jednym z kluczowych elementów platformy Acronis Cyber Protect Cloud jest ochrona antywirusowa z funkcją **Endpoint Detection and Response**. Tradycyjne, wbudowane wcześniej w platformę Acronis rozwiązanie antywirusowe zostało rozbudowane o EDR, co pozwala na bieżące monitorowanie i analizę wykrytych incydentów bezpieczeństwa oraz szybkie reagowanie na nie. Klienci końcowi lub partnerzy MSP mogą śledzić aktywność w środowisku IT, analizować podejrzane zachowania oraz podejmować odpowiednie działania w celu zabezpieczenia systemów.

Mechanizm EDR dostępny na platformie Acronis Cyber Protect Cloud zapewnia zaawansowane funkcje, jak analiza behawioralna, wykrywanie zagrożeń w czasie rzeczywistym, raportowanie incydentów i izolacja złośliwego kodu. To umożliwia dostawcom usług zarządzanych skuteczną ochronę klientów przed ransomware czy zaawansowanymi atakami typu phishing.

Partnerzy mogą też zaoferować użytkownikom pakiet Advanced DLP, który zapewnia ochronę danych osobowych i poufnych dokumentów przed wyciekiem ze stacji roboczych. Rozwiązanie to, bazujące na regułach polityki bezpieczeństwa, nieustannie analizuje przepływ informacji przez sieć oraz weryfikuje dane zapisywane na nośnikach wymiennych, w tym pendrive'ach.

Gwarantowana ciągłość pracy

Kolejnym ważnym elementem platformy Acronis Cyber Protect Cloud jest usługa **Advanced Disaster Recovery**. Umożliwia ona wykonywanie kopii zapasowych obrazów systemów operacyjnych Windows i Linux, zainstalowanych aplikacji oraz plików użytkowników do repozytorium Acronis Cloud Storage. W przypadku awarii dysku takiego komputera, poważnego błędu oprogramowania lub powodzenia ataku cyberprzestępców (np. zaszyfrowania danych przez ransomware), kopia takiego serwera może być uruchomiona w postaci wirtualnej maszyny bezpośrednio w chmurze Acronis.

Przywrócenie takiego środowiska do pracy bezpośrednio z centrum danych producenta następuje bardzo szybko, co minimalizuje ryzyko przestoju i związanych z nim strat. Administratorzy zaś zyskują dodatkowy czas na bezstresowe przywrócenie komputera do pracy – na podobnym lub innym sprzęcie. Bardzo korzystny dla firm jest też w tym przypadku charakterystyczny dla usług chmurowych abonamentowy model cenowy – nie muszą inwestować w drogą infrastrukturę disaster recovery, która nie przyczynia się do wzrostu zysku firmy, a jedynie stanowi koszt ubezpieczenia przed stratami.

Platforma Cyber Protect Cloud może być wykorzystywana bezpośrednio przez użytkowników lub posłużyć partnerom do świadczenia usług. Autoryzowanymi dystrybutorami rozwiązań Acronis w Polsce są: Also, APN Promise, Clico, Dagma, Ingram Micro oraz Systemy Informatyczne ITXON.

Dodatkowe informacje dla partnerów:
Dariusz Mumot, Senior Solutions Engineer, Acronis,
dariusz.mumot@acronis.com

Ankieta CRN.pl: branża w cieniu zwolnień

Chociaż większość uczestników naszej ankiety ani myśli o zwalnianiu pracowników, to trudno uznać, że sytuacja na branżowym rynku pracy jest stabilna.

■ *Tomasz Gołębiowski*

Sytuacja na rynku pracy jest postrzegana różnie, w zależności od punktu widzenia. Ten, który ma pracodawca, wcale nie musi być tożsamy z odczuciami pracownika i często tak właśnie bywa. Niemniej obie „strony" powinny trzymać kciuki za dobrą sytuację gospodarczą, bo jeśli jest ona zła, to wcześniej czy później skutkuje to bezrobociem. A chociaż w okresie wysokiego poziomu bezrobocia pracodawcom łatwiej pozyskać pracowników, to z drugiej strony maleje siła nabywcza społeczeństwa, a biedniejsi konsumenci to biedniejsze firmy – i koło się zamyka. Przy czym akurat branża IT ma to szczęście, że w trudnych czasach cześć przedsiębiorców posiłkuje się właśnie technologiami, celem ograniczenia kosztów czy zwiększenia wydajności, bądź obu tych kwestii jednocześnie. Jak widać, w tej branży czasem gorzej oznacza lepiej i na odwrót.

Ten nieco przydługi wstęp był potrzebny w kontekście niejasnych wniosków, które płyną z wyników naszej sondy na portalu CRN.pl na temat szukania (lub nie) pracowników. Z naszych danych wynika, że co czwarta firma IT prowadzi rekrutację na wiele różnych stanowisk, zaś nieco powyżej 30 proc. na kilka specjalistycznych stanowisk. Z kolei żadnych rekrutacji nie prowadzi obecnie 21 proc. pytanych. W sumie zatem nie jest źle, skoro blisko 80 proc. firm nie prowadzi żadnych zwolnień. Z drugiej strony żegna się z pracownikami na wybranych stanowiskach 13 proc. firm IT, podczas gdy kolejne 8 proc. prowadzi właśnie zwolnienia grupowe. Biorąc to wszystko pod uwagę trudno uznać, że sytuacja na branżowym rynku pracy jest stabilna.

Z ankiety CRN.pl wynika poza tym, że najtrudniej obecnie pozyskać z rynku specjalistów od cyberbezpieczeństwa (42 proc. wskazań). Aż 34 proc. respondentów przyznaje, że ciężko im znaleźć dobrych fachowców na każde stanowisko, a nie ma problemów ze znalezieniem właściwych osób jedynie 12 proc. firm IT. Co ciekawe, tylko 10 proc. pytanych ma kłopoty z zatrudnieniem nowych programistów, a w przypadku specjalistów od zrównoważonego rozwoju odsetek ten wynosi zaledwie 2 proc. (w tym ostatnim przypadku zapewne wynika on z niskiego zapotrzebowania i faktu, że niewielu przedsiębiorców stać na finansowanie takiej właśnie funkcji w ich firmach).

Jakich specjalistów najtrudniej obecnie pozyskać z rynku?

Źródło: CRN.pl

Wyzwania rosną

Kłopoty ze znalezieniem specjalisty ds. cyberbezpieczeństwa mogą się pogłębić w związku z obawami, jakie polskie firmy żywią w w stosunku do nowych unijnych regulacji w tym zakresie. Z danych IDC wynika, że aż 34 proc. firm w Europie z dużym niepokojem przygląda się regulacjom w zakresie cyberbezpieczeństwa (na drugim miejscu są wymagania związane z zapewnieniem suwerenności danych, a na trzecim – ze zrównoważonym rozwojem). W Polsce przepisy dotyczące cyberodporności są wręcz zmorą przedsiębiorców i wysuwają się na pierwszy plan. Chodzi głównie o NIS2 (wprowadza regulacje dotyczące infrastruktury krytycznej) oraz DORA (obejmuje sektor finansowy i firmy świadczące usługi ICT oraz infrastrukturalne dla podmiotów z sektora finansowego). Dla wielu firm oznaczają one kosztowne obowiązki i wyzwania związane z koniecznością dostosowania się do wielu różnych wymogów w określonym terminie.

Cyberodporność staje się zmorą.

Największy problem mają przedsiębiorstwa, które wcześniej nie podlegały żadnym regulacjom w zakresie cyberbezpieczeństwa, a dyrektywa NIS2 to zmienia, rozszerzając wymagania o kolejne sektory gospodarki i podmioty różnej wielkości. Do stosowania nowej dyrektywy będą zobowiązane również mikro- i małe przedsiębiorstwa, które spełnią kryteria dyrektywy, wskazujące na ich kluczową rolę dla społeczeństwa, gospodarki lub określonych sektorów lub typów usług.

Tymczasem według danych DESI 2022 w Polsce brakuje 50 tys. osób specjalistów IT z, czego nawet 20 proc. stanowią eksperci ds. cyberbezpieczeństwa.

W ankietach wzięło udział 405 osób.

Nie od razu AI zbudowano

Producenci i ich partnerzy, którzy postawią na spokojny, ale konsekwentny rozwój działań wokół AI, w dłuższej perspektywie na tym skorzystają.

Sztuczna inteligencja znalazła się na świeczniku. Firmy w różnych branżach prześcigają się w szukaniu sposobów na wykorzystanie możliwości AI w swoich produktach i usługach. Obietnica, jaka się z tym wiąże, a która dotyczy dostarczania spostrzeżeń, automatyzacji zadań i optymalizacji operacji jest niezaprzeczalnie ekscytująca. Płynące z tego korzyści operacyjne pomogłyby złagodzić niedobór talentów, który od kilku lat nęka kanał sprzedaży IT, jak też poprawić rentowność.

Jednak chcąc znaleźć się wśród liderów innowacji w zakresie AI, niektóre firmy wykraczają poza swoje możliwości, generując szum medialny w celu uzyskania krótkoterminowych zysków. Według niedawnego raportu FactSet wspominanie o sztucznej inteligencji podczas rozmów o wynagrodzeniu stało się najnowszą taktyką zwiększania wycen akcji. Ceny akcji spółek z S&P 500, które odwołują się do sztucznej inteligencji, odnotowały w tym roku lepsze wyniki niż spółki spoza „świata" AI. Tego rodzaju „pranie sztucznej inteligencji" może przynieść krótkoterminowe korzyści i poprawić wyniki giełdowe, ale ostatecznie zaszkodzi branży technologicznej i – co za tym idzie – kanałowi sprzedaży.

Partnerzy, starając się zrozumieć rzeczywiste możliwości rozwiązań AI, opierają się na marketingowych przekazach producentów. Dlatego „pranie sztucznej inteligencji" zamazuje różnicę między produktami opartymi na prawdziwej sztucznej inteligencji a tymi, które są po prostu modnymi hasłami. Partnerzy, nie wiedząc, które oferty rzeczywiście zapewniają wymierną wartość ich firmom i klientom, będą marnować czas na rozwiązania, które nie spełnią sztucznie napompowanych oczekiwań.

Przerabialiśmy to już wiele razy. Przez lata dostawcy, których oferta nie miała nic wspólnego z cyberbezpieczeństwem, przekonywali o zdolności swoich produktów i usług do ochrony sieci i danych. Kiedy przetwarzanie w chmurze weszło do głównego nurtu, widzieliśmy, jak dostawcy ścigają się ze sobą, opowiadając o swoich możliwościach w chmurze. A kiedy smartfony uczyniły świat mobilnym, byliśmy świadkami, jak dostawcy chwalili swoją ofertę dostępu do danych za pośrednictwem aplikacji mobilnych. Trudno też wyprzeć z pamięci, jak blockchain miał zmienić świat dzięki otwartym księgom rachunkowym i nienaruszalnej integralności. Nie wszystkie takie twierdzenia były nieważne, ale wiele z nich było rażąco przedwczesnych lub wprowadzających w błąd.

> Przerabialiśmy to już **wiele razy.**

W przypadku partnerów handlowych identyfikacja dostawców, którzy dysponują prawdziwymi możliwościami sztucznej inteligencji, wymaga spojrzenia poza marketingowy bełkot. Prawdziwa innowacja w zakresie AI wymaga dużych inwestycji w infrastrukturę danych, talenty inżynieryjne i moc obliczeniową. Rozwiązania promowane jako „oparte na sztucznej inteligencji" bez idących za tym dowodów powinny budzić sceptycyzm.

„Pranie sztucznej inteligencji" stwarza również ryzyko, że partnerzy handlowi będą na wyrost obiecywać swoim klientom korzyści związane ze sztuczną inteligencją. A jeśli podstawowym rozwiązaniom brakuje solidnej funkcjonalności sztucznej inteligencji, partnerzy nie są w stanie zapewnić oczekiwanych rezultatów. To niszczy wiarygodność i zaufanie. Partnerzy powinni ustalić odpowiednie oczekiwania dotyczące sztucznej inteligencji, jasno określając rzeczywistą dojrzałość sztucznej inteligencji danego producenta. Ponadto „pranie AI" spowalnia jej szersze przyjęcie. Kiedy początkowe wdrożenia nie przynoszą rezultatów, klienci odrzucają sztuczną inteligencję jako technologię przesadzoną, która „nie dowozi" w świetle składanych obietnic.

Tymczasem konstruktywne opinie na temat ograniczeń AI zostają zagłuszone przez nadmierny szum informacyjny wokół dostawców. Praktyczny postęp w zakresie sztucznej inteligencji wymaga uczciwej oceny bieżących możliwości i wyzwań. Rewolucja AI przyniesie ogromną wartość, ale wymaga cierpliwości. Prawdziwa zmiana wymaga trwałego zaangażowania.

Nie oznacza to, że dostawcy nie mogą wsiąść do pociągu AI, ale powinni oprzeć się przedwczesnym, rewolucyjnym obietnicom, które mogą pokrzyżować ich długoterminowe wysiłki. Kanał partnerski również powinien unikać nierealistycznych oczekiwań i szukać dostawców niezachwianie podążających ścieżką AI. Powolny, ale stały postęp może nie trafić na pierwsze strony gazet, tak jak to ma miejsce w ramach szumu informacyjnego wokół sztucznej inteligencji, jednakże doprowadzi do prawdziwych zmian biznesowych. I na ten scenariusz warto stawiać.

Larry Walsh
CEO oraz Chief Analyst w Channelnomics, firmie analitycznej specjalizującej się w kanałach sprzedaży i doradztwie dla producentów, dystrybutorów i integratorów IT. Autor jest również prowadzącym podcast „Changing Channels" i wydawcą magazynu „Channelnomics Quarterly".
Kontakt: lmwalsh@channelnomics.com.

Fot. Adobe Stock

Wykorzystanie AI w rekrutacji

„Powstaje właśnie technologia, dzięki której sztuczna inteligencja będzie wiedzieć jakich odpowiedzi powinni udzielać kandydaci dobrze dopasowani do danego stanowiska" - mówi Tomasz Miller, IT Managing Consultant w Yard Corporate.

CRN W jakim zakresie wykorzystywana jest sztuczna inteligencja w rekrutacji?

Tomasz Miller Sztuczną inteligencję w rekrutacji można wykorzystywać na różne sposoby w celu optymalizacji pracy. Najbardziej popularne jest dodawanie modułów AI do systemów ATS – jest to rozwiązanie rekrutacyjne pozwalające śledzić proces kandydata na poszczególnych etapach rekrutacji. Na rynku dostępne są także systemy pozwalające analizować CV względem prowadzonego projektu rekrutacyjnego. Wystarczy wprowadzić pełny opis stanowiska – wymagania, zakres obowiązków, a narzędzie AI będzie weryfikować kandydatów w bazie i oceniać, czy dana osoba pasuje do wymagań, czy też nie. Narzędzia AI wpływają nie tylko na elementy, które są stricte związane z pracą w HR, ale także na te bieżące zadania, jak chociażby sporządzanie sprawozdań. Z naszych notatek, które są często zlepkiem słów czy bullet pointami, asystent może stworzyć bardzo ładne podsumowanie spotkania z listą zadań do wykonania. Takie rozwiązanie niezwykle ułatwia pracę w wielu zawodach.

> W naszej branży rozwiązania AI **zrewolucjonizowały pracę.**

CRN Czy to prawda, że CV pracowników w dużym stopniu przeglądają algorytmy, a nie ludzie?

AI Candidate Matching to technologia, która jest dopiero wdrażana, nie jest jeszcze popularna i powszechnie używana, ale jest przyszłościowa. Na chwilę obecną algorytmy nie działają tak dobrze, że możemy w stu procentach się na nie zdać, ale już na tym etapie wdrożenia ułatwiają selekcję kandydatów. Pamiętajmy, że na ogłoszenia potrafi napływać bardzo dużo CV. Ich selekcja jest żmudna i monotonna. Każde z nich trzeba otworzyć, przeczytać i przeanalizować. Czynność tę pozwalają zautomatyzować algorytmy, które wyodrębniają kandydatów spełniających oczekiwania przyszłego pracodawcy.

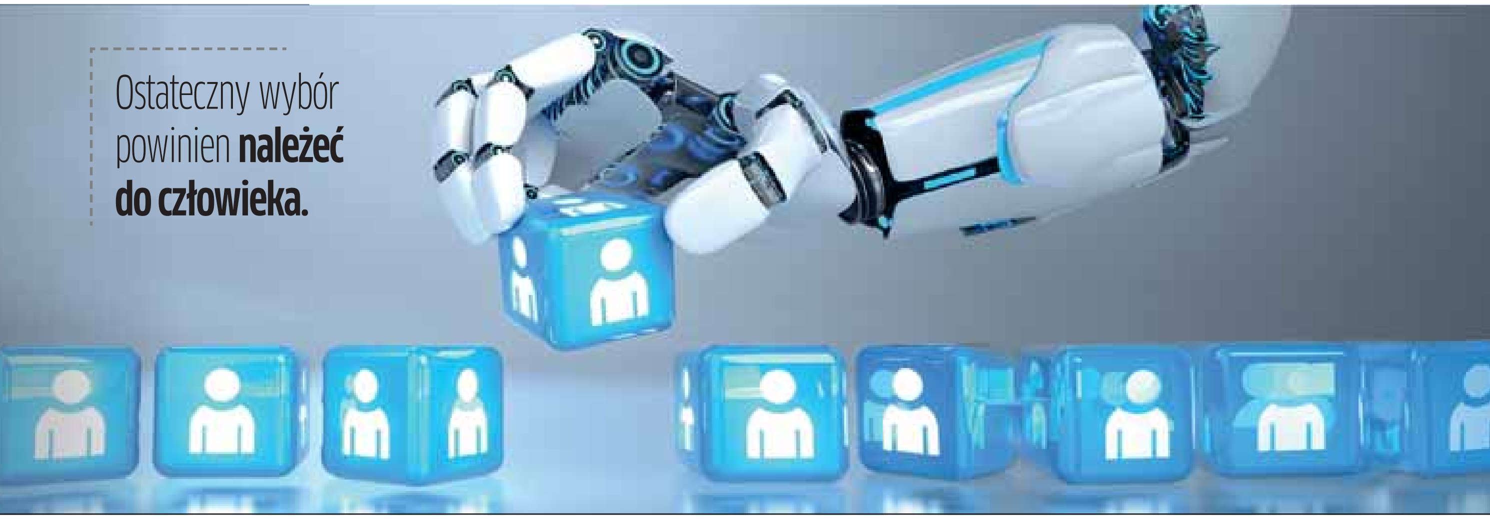
CRN W jaki sposób przygotować CV, aby algorytmy AI lepiej przeprocesowały naszą kandydaturę?

Najnowsze modele językowe są nauczone tego, by dobrze rozumieć tekst pisany, dlatego niezwykle ważne jest, aby w CV zawrzeć jak najwięcej istotnych informacji. Podstawą będą dokładne nazwy stanowisk. Jeśli ktoś ma wpisane, że jest np. Software Developerem, to powinien dopisać, w jakiej dokładnie technologii pracuje. Brak takiej informacji może być mylny dla algorytmu, który odrzuci kandydaturę. Warto wpisywać jak najwięcej słów kluczowych – nazw baz danych, narzędzi czy frameworków, z którymi się pracowało. Istotne jest również podawanie dokładnych dat rozpoczęcia i zakończenia nauki oraz pracy. To pozwoli algorytmom przeanalizować długość okresu edukacji i zatrudnienia. Im większa ilość informacji, tym większe szanse odpowiedniego dopasowania kandydata do stanowiska. Sztuczna inteligencja do analizy potrzebuje danych, im są one bogatsze, tym bardziej rosną realne szanse zdobycia zatrudnienia przez danego kandydata. Dobre CV powinno być zwięzłe, ale zawierające maksymalną ilość informacji.

CRN Czy AI jest w stanie zweryfikować nasze kompetencje, zarówno miękkie, jak i twarde?

Kompetencje twarde, takie jak umiejętność programowania czy korzystania z konkretnych programów AI, jest zdecydowanie w stanie przeanalizować na podstawie informacji zawartych w CV i po analizie danych z wcześniej przygotowanego testu. Oczywiście w następnej kolejności musi to skorygować rekruter. Jednak na etapie wstępnym – tak, jak najbardziej sztuczna inteligencja jest w stanie zweryfikować kompetencje twarde. Jeżeli chodzi o te miękkie, to również są takie możliwości. Jeszcze przed obecnym rozkwitem wszystkich aplikacji AI były dostępne narzędzia, które na przykład na podstawie nagrań wideo i audio potrafiły ocenić, czy dana osoba odpowiadając na pytania stresuje się, szuka odpowiedzi w głowie, czy wie, co konkretnie chce powiedzieć. Powstaje właśnie technologia, dzięki której sztuczna inteligencja będzie wiedzieć, jakich odpowiedzi powinni udzielać kandydaci dobrze dopasowani do danego stanowiska. Wykorzystuje ona rekomendacje ekspertów oraz korzysta z przetworzonych wcześniej artykułów naukowych, które mówią, jakie cechy powinni wykazywać na przykład dobrzy liderzy, handlowcy czy osoby na stanowiskach mocno technicznych. Takie narzędzie pozwoli nam w czasie rzeczywistym ocenić, czy konkretna osoba spełnia kryteria oferty zatrudnienia.

Fot. archiwum



CRN Czy sfera onboardingu, zarządzania rozwojem, kompetencjami zostanie zagospodarowana przez AI?

Jestem przekonany, że tak. Już w tej chwili firmy pracują nad takimi rozwiązaniami. Wystarczy znanemu nam doskonale ChatGPT dać dostęp do informacji firmowych, takich jak chociażby ścieżki rozwoju, regulaminy, aby w szybki sposób udzielał odpowiedzi na pytania pracowników. Dla przykładu, aby zgłosić chęć wymiany laptopa nie trzeba będzie szukać informacji w materiałach zawartych w firmowej bazie wiedzy, wystarczy zadać pytanie, a bot od razu nam odpowie, że tym zajmuje się ta a ta osoba z tego a tego działu. Takie rozwiązania znacznie ułatwiają bieżącą pracę.

CRN Czy kierunki rozwoju istniejących zespołów w firmie będzie dyktowała AI? Przykładowo, dobór brakujących kompetencji do zespołu?

W budowaniu zespołu niezwykle ważny jest czynnik ludzki. W codziennej pracy istotne jest dopasowanie osobowościowe pracowników, którzy spędzają wspólnie wiele godzin każdego dnia. Sztuczna inteligencja wskaże pulę kandydatów spełniających wymogi danego stanowiska, przeanalizuje lata doświadczenia zawodowego, jednak ostateczny wybór będzie należał do człowieka, który kandydata dopasuje również pod kątem personalnej współpracy w zespole i z zespołem.

CRN Jakie jeszcze jest zastosowanie AI w zakresie rekrutacji i zarządzania zasobami ludzkimi? W jakim kierunku przewidujecie rozwój tej technologii w waszej branży?

Firmy prześcigają się w tworzeniu nowoczesnych rozwiązań ułatwiających pracę, pozwalających osiągnąć lepszą efektywność oraz wyniki. Śledzimy wszystkie nowo pojawiające się narzędzia i wdrażamy je w Yard Corporate. Jesteśmy firmą wykorzystującą na co dzień sztuczną inteligencję. W naszej branży pojawienie się rozwiązań AI zrewolucjonizowało pracę. Dynamika jest tak duża we wdrażaniu kolejnych i kolejnych rozwiązań, że trudno jest prognozować, co będzie za rok, nie mówiąc już o perspektywie kilku lat. Z całą pewnością nasza praca będzie bardziej zautomatyzowana, więcej zadań będzie wykonywała sztuczna inteligencja. Na pewno będzie to tworzenie mejli, pisanie podsumowań spotkań, obrad czy analizowanie CV. Dzięki temu będziemy mogli skupić się na czynniku ludzkim – na pracy, którą dobrze może wykonać tylko człowiek.

CRN Algorytmy AI nie są jeszcze doskonałe, mogą popełniać błędy. Nie boicie się, że proces analizy wskaże nieodpowiedniego kandydata? Wskaże złego, a odrzuci dobrego?

To jest pytanie, które zadaje sobie wiele osób. AI nie zastąpi człowieka, ponieważ popełnia błędy. Bardzo ważne jest to, aby rozwiązania sztucznej inteligencji traktować jako narzędzia, które ułatwiają naszą pracę, a nie tę pracę zastąpią. Dlatego ewentualne pomyłki AI nie wpływają negatywnie na rekrutacje w Yard Corporate, ponieważ to my ją wykonujemy, a technologia jest tylko i aż wsparciem. W obszarze HR czynnik ludzki jest niezwykle ważny. Nawet najbardziej zaawansowana sztuczna inteligencja nie zastąpi naszej funkcji w zawodzie rekrutera.

CRN W jaki sposób weryfikować wskazania sztucznej inteligencji?

Praca manualna jest nieodłączną częścią naszego zawodu. Gdy potrzebujemy zrobić selekcję kandydatów – z tysiąca osób wybrać dziesięć – to możemy zdać się na research sztucznej inteligencji. Natomiast gdy pula kandydatów jest zdecydowanie mniejsza, to weryfikację musimy przeprowadzić ręcznie, aby właśnie uniknąć ewentualnych błędów AI. Naszym klientom staramy się przedstawić trzech-czterech kandydatów, idealnie dopasowanych specjalistów na dany wakat. Spośród nich klient wybiera tego finalnego.

CRN Czy CV nadal będzie nieodłącznym elementem na linii pracownik-kandydat? Czy z czasem prezentowanie doświadczenia przybierze inną formę?

Już teraz zauważamy, że CV nie zawsze potrzebne jest w trakcie rekrutacji. Na znaczeniu rosną branżowe portale, w szczególności Linkedin. Bardzo dobrze uzupełniony profil zastępuje z powodzeniem klasyczne CV.

CRN Jakie zmiany na rynku rekrutacji pojawią się na przestrzeni 3, 6 i 12 lat?

Rynek IT jest niezwykle dynamiczny, trudno prognozować co będzie za rok, a co dopiero na przestrzeni dwunastu lat. To, w jaki sposób rozwijają się modele językowe, diametralnie zmienia ich użyteczność. Na pewno będzie więcej automatyzacji, której wzrost obserwujemy od lat.

Rozmawiała
Weronika Tymosiak

Efekt Ringelmanna, ??????

Nadal spotykam menedżerów i przedsiębiorców, którzy uważają, że im więcej osób uczestniczy w danym projekcie, tym szybciej zostanie on ukończony. To błąd.

Według Jeffa Bezosa, byłego CEO Amazona, najbardziej produktywne zespoły to te, które da się nakarmić dwoma pizzami. Pracując w Dellu i Samsungu, miałem do dyspozycji dziesiątki zwinnych umysłów. Obecnie w audycji Zaprojektuj Swoje Życie (ZSŻ) współpracuję z 6 osobami. Dwie pizze nam wystarczą. Czy w małych zespołach faktycznie drzemie ogromna siła?

Nadal spotykam menedżerów i przedsiębiorców, którzy uważają, że im więcej osób uczestniczy w danym projekcie, tym szybciej zostanie on ukończony. Tymczasem z doświadczenia wiem, że takie nieskończone powiększanie zespołu może osłabić jego produktywność. Są nawet badania, które wskazują, że niewielkie grupy maksymalizują swój potencjał twórczy. Dzięki niewielkim zespołom zyskujesz większe zaangażowanie, poziom odpowiedzialności wzrasta, a produktywność osiąga nowe wyżyny.

Jeśli chciałbyś zgłębić ten temat, polecam poczytać o efekcie Ringelmanna, znanym też jako efekcie próżniactwa społecznego. Polega na tym, że im więcej osób równocześnie wykonuje jakąś pracę, tym gorszy ostateczny rezultat w porównaniu z sumą wyników poszczególnych osób. Z kolei im mniej osób ze sobą współpracuje, tym łatwiej jest im połączyć siły i realizować założone cele.

W ZSŻ komunikujemy się przez Slack. Z uwagą obserwuję, jak mój zespół wspiera się, rozwiązuje problemy i angażuje we wspólnie określone priorytety. Co więcej, inspirujemy się do działania, znamy swoje talenty i dostrzegamy wzajemny potencjał. Taka bliskość połączona z efektywnością nie byłaby możliwa w 30-osobowej drużynie. Dlatego dostrzegam ogromny potencjał w małych zespołach. Poniżej kilka niezaprzeczalnych zalet takich grup.

> Indywidualny wysiłek **maleje, kiedy zespół się zwiększa.**

Duże zaangażowanie

W artykule „Why Small Teams Are Better Than Large Ones" Jacob Morgan pisze, że pracownicy są bardziej zaangażowani i usatysfakcjonowani z osiągnięć, gdy mają możliwość działania w niewielkich grupach. Małe zespoły zapobiegają „społecznemu próżniactwu", gdzie indywidualny wkład jest postrzegany jako mniej wartościowy ze względu na liczbę osób wykonujących to samo zadanie. Indywidualny wysiłek maleje wraz ze wzrostem wielkości zespołu. Co więcej, członkowie niewielkich grup często mają większą kontrolę nad swoją pracą i bardziej angażują się w proces podejmowania decyzji.

Efektywna komunikacja

Na pewno nie zdziwi Cię fakt, że efektywniej komunikujemy się w mniejszych grupach niż w większych. Świetnie obrazuje to prawo Brooksa – im więcej osób pracuje nad projektem, tym komunikacja staje się trudniejsza. Co więcej, czas ukończenia zadania znacznie się wydłuża.

Pracując w niewielkich zespołach, jesteśmy bardziej świadomi tego, za co każdy jego członek jest odpowiedzialny. Dzięki temu łatwiej zrozumieć, jak nasza praca wpisuje się w szerszy plan działania. Im bardziej pokaźny zespół, tym komunikacja staje się trudniejsza. Zaczyna wkradać się chaos i zagmatwanie. Świetnie podsumowuje to J. Richard Hackman: „Big teams usually wind up wasting everybody's time".

Innowacyjność

Małe zespoły są skuteczne, gdyż skłaniają swoich członków do bardziej elastycznego

Fot. Adobe Stock

czyli małe jest piękne

myślenia i innowacyjności. Ponieważ każda z osób jest zazwyczaj odpowiedzialna za kilka zadań, istnieje większa potrzeba wychodzenia poza schematy i podejmowania, czasem nieoczywistych, decyzji, które prowadzą do osiągnięcia celu.

Wsparcie, czyli więcej znaczy mniej

Kolejną zaletą niewielkich grup projektowych jest wzajemne wsparcie. Tyczy się to nie tylko członków zespołu, ale także lidera, który może poświęcić więcej czasu poszczególnym osobom.

Ułatwia to przeciwdziałanie czynnikom stresogennym i promowanie sukcesu każdej z osób zaangażowanych w projekt.

Mniejsze zespoły to większa odpowiedzialność za podejmowane działania. To także autonomia i elastyczność. Przeprowadzono nawet badanie, w którym dwu- i czteroosobowe zespoły miały za zadanie zbudować konstrukcję z klocków Lego. Wynik? Dwuosobowy zespół ukończył zadanie w czasie krótszym o 36 proc.

Rola lidera

Członkowie niewielkich zespołów mają w sobie więcej energii do działania. Skutkuje to większą wydajnością i skutecznością. Jon R. Katzenbach, współautor książki „The Wisdom of Teams”, zauważa, że niewielkie zespoły dają liderom większe możliwości wykazania się. Jego zdaniem maksymalne wykorzystanie potencjału drzemiącego w takich zespołach zależy od pięciu rzeczy: jasno sformułowanego i przekonującego celu działania; jasno określonych celów do osiągnięcia; odpowiedniego zestawu kwalifikacji u członków zespołu; wzajemnej odpowiedzialności; zdolności przekazywania roli lidera między członkami zespołu, w zależności od konkretnych okoliczności.

Pracując z małymi zespołami, pamiętaj, aby zapewnić swoim ludziom odpowiednie kanały komunikacji. Nie zapominaj też, że jesteś nie tylko liderem, ale też częścią grupy. Bądź dostępny i wspierający. Doceniając zaangażowanie, kreatywność i czas, który wkładacie w wasze działania, nadajesz siłę napędową grupie.

Podsumowanie

Wraz ze wzrostem zaangażowania, innowacyjności i produktywności, zalety „odchudzania” zespołu w Twojej firmie wydają się oczywiste. Zależy Ci na pracownikach i menedżerach, na których możesz polegać. Dlaczego więc nie zmaksymalizować ich potencjału, aby to osiągnąć?

Oczywiście wszystko sprowadza się do tego, co najlepiej sprawdza się w Twoim biznesie. W moim praca z małym zespołem ułatwia mi prowadzenie firmy. Postaraj się obiektywnie określić, ile osób potrzebujesz do pracy nad danym projektem. Z kim musisz się komunikować? Jak dużą autonomię powinni mieć członkowie zespołów?

W zależności od tego, jak bardzo jesteś zadowolony z poziomu produktywności i wzrostu biznesowego, warto być otwartym na zmiany. Rozważ rozpoczęcie pracy z mniejszymi zespołami.

Maciej Filipkowski

Autor jest aktywnym inwestorem i twórcą audycji „Zaprojektuj Swoje Życie” (Podcast Biznesowy Zaprojektuj Swoje Życie Maciej Filipkowski. Porady dla Przedsiębiorców i Wywiady. (zaprojektujswojezycie.pl).

Narzekanie, wypalenie, depresja

Czy i jak wspierać pracowników w kryzysie?

Bez względu na to, co jest źródłem kryzysu pracownika, objawy na zewnątrz będą podobne.

Zaburzenia psychiczne to zagadnienie odmieniane obecnie przez wszystkie przypadki. Fakt ten nikogo jednak nie dziwi, bowiem od dłuższego czasu żyjemy pod wpływem wielu negatywnych bodźców i wydarzeń. Według badań Światowej Organizacji Zdrowia 20 proc. populacji Ziemi chociaż raz w życiu zmierzy się z depresją. Momentem, który nasilił i tak mało optymistyczne statystyki, była pandemia. W ujęciu wspomnianej organizacji również ona zebrała swoje żniwo. Szacuje się, że przed Covid-19 co dziesiąta osoba zgłaszała swojemu menadżerowi trudności emocjonalne. Dziś liczba ta wynosi 30 proc.

Stany Zjednoczone, Kanada, Wielka Brytania i Nowa Zelandia to kraje, które przodują w systemach wsparcia psychicznego w miejscu pracy. Z raportów tych firm wynika, że 1 dolar zainwestowany w działania mające na celu poprawę i wsparcie zdrowia psychicznego pracowników, to 4 dolary zwrotu kosztów dla firmy. W skrajnych przypadkach kwota ta dochodzi nawet do 17 dolarów.

Naszą odporność psychiczną **buduje samoocena.**

Pracownicy, którzy otrzymują wewnątrz firmy wsparcie w walce z chorobą, mają średnio o 30 proc. krótsze zwolnienia lekarskie. Ponadto w instytucjach, gdzie psychoedukacja, well-being i działania prewencyjne są na zaawansowanym poziomie, ludzie chorują o 50 proc. rzadziej. Wynika to z tego, że chroniczny stres ma niebagatelny wpływ na nasz układ odpornościowy. Z ekonomicznego punktu widzenia dbanie o komfort psychiczny pracowników zwyczajnie się opłaca.

Jak rozpoznawać pracownika w kryzysie?

Bez względu na to, czy pracownik przechodzi depresję, trudny rozwód czy też obarczony jest opieką nad chorym bliskim, objawy na zewnątrz będą podobne. Nie musimy mieć wiedzy z psychopatologii i umieć rozróżniać zaburzeń afektywno-dwubiegunowych od ADHD, aby wyłapać objawy. Z rozpoznaniem zmiany w zachowaniu pracownika menadżerowie zwykle dobrze sobie radzą, ponieważ taka osoba najczęściej ma po prostu mniej energii, zaczyna popełniać błędy, które sygnalizuje zespół, ma problemy ze skupieniem się w czasie spotkań, zamyśla się, nie słucha, jest zdekoncentrowana. Czerwoną flagą jest huśtawka emocjonalna, fakt, że ktoś staje się kłótliwy, agresywny, nie radzi sobie ze stresem i jest pobudzony, albo odwrotnie – wpada w płacz po konstruktywnym feedbacku.

Wypalenie…

Wypalenie zawodowe rozumiane jest jako reakcja organizmu na długotrwały stres wynikający z pełnionych obowiązków zawodowych. Powstaje ono zazwyczaj na skutek przeciążenia pracą, podejmowania odpowiedzialności za trudne zadania, intensywne kontakty społeczne, jak też w wyniku wykonywania monotonnych obowiązków. Skutkiem wypalenia zawodowego jest szereg nieprzyjemnych konsekwencji związanych ze stanem psychicznym czy emocjonalnym, jak również zdrowiem fizycznym, kontaktami społecznymi, wynikami pracy, a nawet sensem życia.

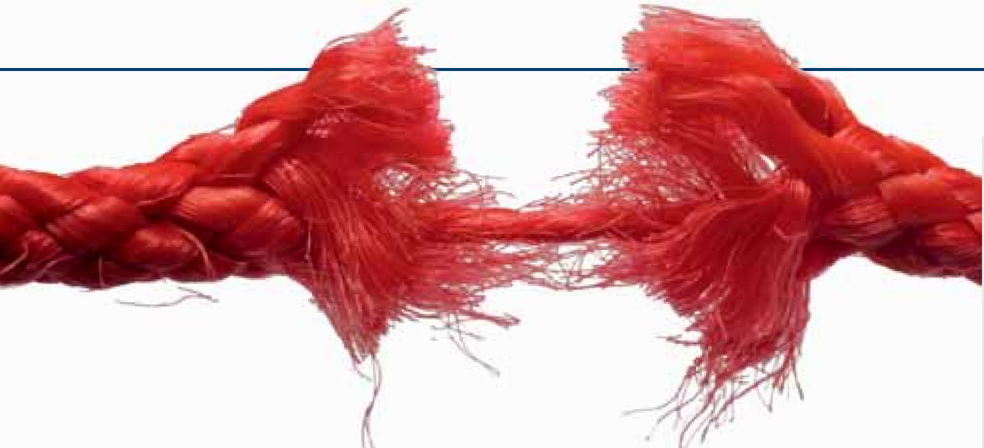
Zwykle wypalenie rozwija się od prostych stresorów, które najczęściej zdarzają się w pracy. Stres zaczyna się od wyobrażania sobie, że coś złego może się wydarzyć. Jeśli w organizacji pracownicy są przytłoczeni liczbą zadań, brakuje wsparcia, jest nieprzyjazna atmosfera, nie ma kultury wdzięczności, to pracownik żyje w chronicznym stresie. To powoduje, że ma podwyższony poziom adrenaliny i kortyzolu, a w momencie, gdy kortyzolu jest za dużo i jego wysoki poziom utrzymuje się bez przerwy, to uszkadza w pniu mózgu ośrodki, które są odpowiedzialne za dopaminę i serotoninę. Dopamina jest neuroprzekaźnikiem odpowiedzialnym za motywację, więc jeżeli pień mózgu przestaje ją wydzielać, to przestaje nam się chcieć pracować. To objaw zarówno wypalenia zawodowego, jak i depresji .

Serotonina to główny transmiter w korze przedczołowej. To tam znajdują się ośrodki odpowiedzialne za podejmowanie decyzji, analizę, kreatywność, pamięć, samokontrolę. Chroniczny stres będzie prowadził do sytuacji, w której nie mamy nowych pomysłów, nie potrafimy myśleć kreatywnie, spada koncentracja i zaczynamy popełniać błędy. Na zaawansowanym etapie wypalenia zawodowego pojawiają się objawy psychosomatyczne, ponieważ stres uszkadza wiele narządów w naszym ciele. W związku z tym, osobom narażonym na przewlekły stres grozi astma, otyłość, insulinooporność, choroby kardiologiczne, a nawet onkologiczne.

Wypalenie zawodowe a depresja

Objawy depresji i wypalenia zawodowego są bardzo podobne. Należą do nich: zmęczenie, brak motywacji, satysfakcji, niska samoocena. Natomiast jest też podstawowa różnica między tymi stanami. W depresji bowiem człowiek ma zgeneralizowane myślenie negatywne: „ja jestem do niczego, świat jest do niczego, praca jest do niczego, nie widzę żadnej nadziei”. Natomiast w przypadku wypalenia zawodowego człowiek wie, że stan, w którym jest, wynika z pracy zawodowej. Druga rzecz, która różnicuje te dwa sta-

Fot. Adobe Stock



ny, to agresja. Przy wypaleniu zawodowym odnosi się ona do pracy, przy depresji – do wszystkich aspektów życia.

Jak reagować?

Wsparcie pracowników w kryzysie można rozróżnić na prewencyjne i interwencyjne. Jest wiele działań prewencyjnych, które budują odporność psychiczną na poziomie pracownika i firmy. Przede wszystkim kluczowa jest edukacja i wzrost świadomości. Wiedzę tę powinien posiadać menadżer, ale też choć w podstawowym zakresie inni pracownicy. Dlaczego? Bardzo często ludzie zwierzają się w mniej oficjalnych sytuacjach kolegom i koleżankom zza biurka. Istotne jest, aby taki pracownik wiedział jak zareagować, co powiedzieć i komu taką informację przekazać. Im wcześniej rozpoznamy istniejący problem, tym szybsza szansa na wyzdrowienie i poradzenie sobie z problemem. Według badań około 70–80 proc. osób borykających się z zaburzeniami psychicznymi wróci do równowagi i nie będzie miało przewlekłych problemów psychicznych.

Czynnikiem, który buduje naszą odporność psychiczną jest samoocena. Na nią z kolei wpływa atmosfera w pracy, relacje z zespołem, fakt czy otrzymujemy pozytywny feedback, wsparcie merytoryczne itp. To wszystko składa się na działania prewencyjne. Równie istotne jest przekonanie, że jeśli poproszę o pomoc, to ją otrzymam.

Również wśród działań interwencyjnych istnieje wiele możliwości reakcji. Przede wszystkim kluczowe jest wyłapanie problemu, dlatego tak ważna jest wspomniana wcześniej edukacja. Rolą menadżera jest nieudawanie, że tego problemu nie ma. Najlepszym rozwiązaniem jest szczera rozmowa z pracownikiem i zbadanie jego potrzeb w tym zakresie. Są osoby, które będą miały na tyle zasobów wewnętrznych, że poradzą sobie same i będą chciały uniknąć zaangażowania menadżera czy kolegów z pracy. Będą też tacy, którzy wręcz będą oczekiwali rozmowy, wsparcia, zauważenia ich problemu.

Zadaniem menadżera jest stworzenie takiemu pracownikowi warunków do swobodnego przejścia przez proces zdrowienia, danie przyzwolenia na obniżenie produktywności, zaproponowanie bardziej elastycznego czasu pracy. Warto również ustalić z pracownikiem, czy jego problem może być zakomunikowany w zespole. Jeśli jest na to przyzwolenie, należy poinformować zespół, skąd wzięło się nagłe obniżenie wymagań w stosunku do danej osoby tak, aby inni pracownicy nie pomyśleli, że jest to faworyzowanie, a potrafili okazać wsparcie. Warto podkreślić, że to okres przejściowy.

Zakomunikowanie takiej sytuacji w zespole jest również istotne dlatego, że osoby cierpiące na depresję mogą być agresywne i konfliktowe. Często zdarza się, że informacja o chorobie wychodzi na jaw w momencie, jak konflikt z osobą z zaburzeniami eskaluje i informacja o problemie dochodzi do menadżera. Niejednokrotnie dopiero wtedy okazuje się, jakie były prawdziwe powody zachowania danego pracownika. Kiedy pozostali członkowie zespołu wiedzą, z czym zmaga się ich koleżanka lub kolega potrafią zastosować filtr, uargumentować pewne zachowania i być bardziej wyrozumiali.

Menadżer musi jednak pamiętać, że jego rolą nie jest wyręczanie, kontrolowanie i wymyślanie rozwiązań za osobę cierpiącą, tylko wzmocnienie jej i zbudowanie wokół takiego pracownika przestrzeni do pracy nad sobą. Jeśli ustalimy z pracownikiem „plan naprawczy", możemy zrobić „check", ale nie wykonamy zadań za taką osobę. Menadżer nie bierze pełnej odpowiedzialności za to, co pracownik zrobi po przyjściu do domu i czy wykorzysta pomoc, którą mu zaoferowano.

Artykuł powstał na bazie wystąpienia podczas konferencji IT Manager of Tomorrow 2022, zorganizowanej przez Let'sManage IT.

Statystyki: problemy psychiczne to realny problem

- 20 proc. pracowników w Polsce mierzy się z kryzysami natury psychicznej
- 7/10 osób odczuwało podwyższony stres w okresie pandemii
- pierwsze wypalenie zawodowe zwykle zdarza się między 1 a 2 rokiem po studiach
- ryzyko wypalenia zawodowego w sektorze IT wynosi 80 proc.
- 37 proc. Polaków deklaruje, że główny stres, który odczuwają związany jest z pracą

Wypalenie zawodowe: krótki test*

Odpowiadając na poniższe pytanie otrzymasz informacje, czy należysz do grupy osób dotkniętych syndromem wypalenia zawodowego, zagrożonych wypaleniem, a może jesteś osobą, która czerpie pełną satysfakcję z pracy i problem wypalenia Cię nie dotyczy.

- Każdego ranka budzę się wypoczęty/a i chętnie idę do pracy
- Czasami czuję się zestresowany/a i zmęczony/a, ale zazwyczaj jestem zadowolony/a ze swojej pracy
- Często myślę o zmianie pracy, ale nadal chcę robić to, co robię
- Wstaję z łóżka myśląc, że będzie to kolejny głupi dzień w pracy
- Mam dość pracy i ludzie mnie irytują, nienawidzę tego co robię

**Test został oparty na koncepcji Christiny Maslach.*

Małgorzata Wypych
jest prezesem zarządu Mental Health Center.

Po co nam Komisja Europejska?

Zamiast faktycznie stać na straży przestrzegania prawa unijnego KE wybiera te sprawy, które mają charakter polityczny.

Komisja Europejska zwana jest często Strażniczką Traktatów (europejskich). Jedną z jej głównych prerogatyw jest więc czuwanie nad przestrzeganiem przez państwa członkowskie prawa unijnego. Jednak moje dotychczasowe doświadczenia z instytucją skargi do KE nie napawają optymizmem.

Pierwszą skargę do KE złożyłem w 2005 r. i dotyczyła ona niezgodności z prawem unijnym przepisów związanych z odliczeniem VAT w przypadku samochodów osobowych i paliwa. Zanim młyny Komisji rozstrzygnęły kwestię, WSA w Krakowie zdążył skierować sprawę do TSUE, a Trybunał wydać wyrok (sprawa Magoora). Udało się więc tę sprawę wyjaśnić bez ingerencji KE (za to z dużą dozą indolencji po jej stronie).

Naruszenie unijnego prawa **jest ewidentne.**

Niezrażeni tym (wtedy jeszcze jednostkowym) doświadczeniem, dwa lata temu przygotowaliśmy z zespołem MartiniTAX kolejną skargę do KE – tym razem dotyczącą błędnej praktyki w zakresie określania podstawy opodatkowania VAT w przypadku aportu z agio. Praktyka ta, której poziom absurdu powoduje wręcz ból fizyczny, zakłada, że podstawa opodatkowania VAT obejmuje tylko tę część „wynagrodzenia", która dotyczy wartości nominalnej akcji lub udziałów otrzymywanych w zamian za aport. Zatem przykładowo, gdy wniesiemy nieruchomość o wartości 100 milionów aportem i 1 proc. zwiększy kapitał zakładowy, a 99 proc. kapitał zapasowy, podstawa opodatkowania VAT miałaby wynosić jedynie 1 milion, a nie 100 milionów.

Nie trzeba być geniuszem w zakresie VAT, żeby stwierdzić, że koncepcja ta do szczególnie mądrych nie należy, przy czym naruszenie prawa unijnego również jest ewidentne. Żeby potwierdzić istnienie takiej ogólnej praktyki niezgodnej z prawem unijnym przedstawiliśmy 24 wyroki sądowe i 76 interpretacji (czyli praktycznie wszystkie jakie istniały w tym zakresie).

Dostaliśmy jednak taką odpowiedź: „Jednocześnie nie można wykluczyć, że stosowanie tego przepisu w odniesieniu do wkładu rzeczowego mogłoby w niektórych indywidualnych przypadkach stanowić naruszenie prawa UE. Mimo że przedstawił Pan pewną liczbę krajowych wyroków i decyzji administracji podatkowej, nadal uważam, że nie ma wystarczających przesłanek pozwalających Komisji stwierdzić istnienie ogólnej praktyki administracyjnej, która naruszałaby prawo UE".

Można odnieść wrażenie, że zamiast faktycznie stać na straży przestrzegania prawa unijnego KE wybiera te sprawy, które mają charakter polityczny, a przynajmniej są głośne. Niestety aport z agio z tego punktu widzenia nie jest szczególnie sexy... No cóż, nie łudzę się, że Komisja zmieni kiedyś swoje podejście.

Jerzy Martini
Partner i doradca podatkowy
w Kancelarii MartiniTAX.

Fot. Adobe Stock

Decoupling **po amerykańsku**

Amerykańska strategia decouplingu polega na zniechęcaniu świata do prowadzenia interesów z Chinami, a następnie przejmowaniu próżni po konkurencji, która posłusznie podwinęła ogon i się wycofała.

Dziś w niedzielę – wyjątkowo – zostałem w Shenzhen. Tym razem, z powodu tajfunów, nie wybrałem się do Hongkongu. Pierwszy tajfun przeszedł wczoraj, a następny ma przyjść już jutro. Wybrałem się więc na spacer do pobliskiego Parku Liczi, zaledwie 5 minut spacerem od mojego mieszkania.

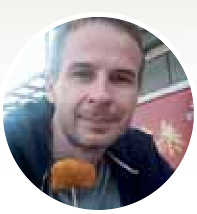
Liczi to średniej wielkości park, o powierzchni 30 ha i bogatej infrastrukturze, a przede wszystkim 500 starymi drzewami liczi. Można tu odnaleźć zaciszne miejsca, aby sobie usiąść przy małym wodospadzie i odpocząć w cieniu albo uczestniczyć w różnych rodzajach aktywności. Poczynając od łowienia ryb (bez żadnych uprawnień), uprawiania ćwiczeń na urządzeniach fitness, gry w siatkę lub tenisa stołowego albo konkurowania w grach planszowych i karcianych. Można też ograniczyć się tylko do odwiedzania zakątków tematycznych, gdzie muzycy grają na tradycyjnych instrumentach, bądź starsze osoby tańczą do muzyki z głośnika albo wykonują ćwiczenia Tai Chi. Można też rozłożyć koc albo namiot i wylegiwać się na kamienistej plaży robiąc dokładnie nic. Interesujące może też być oglądanie drzew i krzewów zaopatrzonych w tabliczki informacyjne i kody QR kierujące do dokładniejszych opisów.

Panuje atmosfera ogólnie rodzinna. Jest bardzo miło i bezpiecznie. Woda pitna jest dostępna za darmo bez ograniczeń. Warunki w również bezpłatnych toaletach bardzo przyzwoite. W ogóle w całych Chinach toalety i woda pitna są dostępne powszechnie i bezpłatnie. Automaty do napojów odpłatnych oferują wodę butelkową (w cenie 1,5 zł za butelkę) i inne napoje, w tym Pepsi w cenie 2,5 zł za puszkę. Jest też jeden jedyny punkt gastronomiczny z lodami i kawą pod marką KFC. To akurat mnie nie dziwi, bo jest zgodne z amerykańską strategią decouplingu, polegającą na zniechęcaniu świata do prowadzenia interesów z Chinami, a następnie przejmowaniu próżni po konkurencji, która posłusznie podwinęła ogon i się wycofała. W sumie mam wielki szacunek dla tak mistrzowskiego posunięcia Amerykanów w obszarze ochrony własnego biznesu. Prawdziwy szacun, bez cienia sarkazmu. No, może z nutą zazdrości…

> Ktoś może się **nieźle zdziwić…**

Marki amerykańskie odnotowują absolutną eksplozję sprzedaży w Chinach. Sam znam kilka osób, które pracują w salonach sprzedaży Apple'a i Nike'a oraz w Starbucksie i KFC. Myślę, że tym samym markom wiedzie się też nieźle w Europie ze sprzedaży chińszczyzny… no bo im przecież wolno. A jeśli ktoś z nas chciałby robić to samo… to może się nieźle zdziwić.

A swoją drogą, podczas wczorajszego tajfunu tylko Subway dowoził jedzenie na zamówienie online. I dzięki temu po raz pierwszy zamówiłem u nich kanapkę i nie żałuję, bo przypomniałem sobie smak szynki – mistrzostwo świata. Teraz codziennie zamawiam w Subwayu kanapkę z szynką!



Arnold Adamczyk
Autor od 2012 roku prowadzi działalność w Chinach i Hong Kongu w zakresie VR/AR/MR oraz edukacji STEM. Specjalizuje się w organizowaniu polskich startupów w Chinach i Hong Kongu.

Dane dobre z natury

„Chcielibyśmy wraz z doprowadzeniem łączy światłowodowych zmodernizować całą naszą infrastrukturę teleinformatyczną. Liczymy na pozyskanie zewnętrznych środków na ten cel" – mówi **Katarzyna Kopiejczyk, zastępca dyrektora ds. administracyjnych w Białowieskim Parku Narodowym (BPN).**

CRN Symbolem Białowieskiego Parku Narodowego jest żubr. Opiekę nad tymi zwierzętami sprawuje działający w ramach Parku Ośrodek Hodowli Żubrów. Z jakich rozwiązań informatycznych korzysta na co dzień?

Katarzyna Kopiejczyk Bardzo pomocne w zarządzaniu populacją żubra są obroże telemetryczne. Dzięki nim możliwe jest tworzenie map pokazujących, po jakim obszarze porusza się stado, jaka jest jego liczebność i aktywność na danym terenie. Można zlokalizować miejsca odpoczynku zwierząt, ocenić ich preferencje siedliskowe, określić czynniki, które mają szczególny wpływ na ich zachowania. Obroża ma wbudowanych kilka modułów. GPS pokazuje lokalizację obroży, GSM wysyła zebrane dane, a moduł radiowy emituje sygnał namierzany przy pomocy anteny i odbiornika. Dzięki niemu możemy w każdej chwili zlokalizować dokładnie każde pojedyncze zwierzę.

CRN Z tego co wiem, od niedawna rejestrujecie też w formie cyfrowej odgłosy Puszczy Białowieskiej...

W ramach inicjatywy Huawei TECH4ALL, Białowieski Park Narodowy, organizacja Rainforest Connection i Huawei wspólnie wdrożyły system monitoringu akustycznego w Puszczy Białowieskiej. Celem tego projektu, jest badanie wpływu zmian klimatu na lokalną bioróżnorodność. System składa się z 70 czujników akustycznych rejestrujących odgłosy przyrody, w tym wokalizacje różnych gatunków zwierząt i ptaków. Wykorzystywane do tego urządzenia AudioMoth Edge są zaawansowanymi rejestratorami dźwięku o pełnym spektrum. Wychwytują zarówno częstotliwości słyszalne, jak i ultradźwiękowe, które są automatycznie zapisywane na kartach SD w formie nieskompresowanej. Zebrane w ten sposób dane są następnie przesyłane do platformy chmurowej w celu ich analizy za pomocą oprogramowania korzystającego ze sztucznej inteligencji. Do przesyłania danych służą specjalne urządzenia marki Guardian. Są one zasilane energią słoneczną, mają wbudowane mikro-odbiorniki i anteny do przesyłania danych audio do chmury za pośrednictwem sieci GSM. Dzięki temu systemowi możemy stale monitorować aktywności dzikich zwierząt w puszczy.

> Planujemy **wymianę** serwerów wraz z ich **wirtualizacją.**

CRN Czy jeszcze w jakiś inny sposób rejestrujecie oznaki życia w naturze?

Tak, podejmujemy wiele działań w celu monitorowania naszych terenów i zbierania danych dotyczących znajdujących się tam gatunków. Mamy fotopułapki, mamy kamery termowizyjne, mamy podgląd na zwierzęta na wolności za pośrednictwem kamer telewizyjnych, mamy specjalne mikrofony do nagrywania i odsłuchu dźwięków ptaków. Chcemy wiedzieć, jakie ptaki w jakich miejscach u nas żyją i jak się zachowują. Zebrane informacje umieszczane są w bazach danych i przetwarzane przez różne działy czy ośrodki, na przykład Pracownię Naukową, Zespół do spraw Ochrony Przyrody, Ośrodek Edukacji Przyrodniczej.

CRN Białowieski Park Narodowy ma powierzchnię 10,5 tysiąca hektarów, a jego teren jest w całości zalesiony. W jaki sposób narzędzia informatyczne pomagają w utrzymaniu nadzoru nad tak dużą przestrzenią?

Teren Parku podzielony jest na sześć obwodów ochronnych, którymi opiekują się pracownicy terenowi. Mają oni do dyspozycji specjalną aplikację zainstalowaną na służbowych smartfonach. Służy ona zarówno do lokalizacji własnego położenia pracownika poprzez dostęp do mapy terenu, jak i do wprowadzania danych monitoringowych. Wśród zbieranych informacji są dane dotyczące lokalizacji stwierdzonego gatunku inwazyjnego, oznaczenia występowania niebezpiecznych drzew przy szlakach turystycznych, stwierdzenie zaśmiecania terenu, wandalizmu czy też palenia ognisk. Możliwe jest też dodawanie notatek z przeprowadzonego patrolowania terenu oraz tworzenie raportów na podstawie wprowadzonych danych. Aplikacja działa zarówno w trybie online, jak i offline. Po znalezieniu się smartfonu w zasięgu sieci komórkowej, zgromadzone dane przesyłane są automatycznie do serwera głównego oraz na bieżąco aktualizowane.

Fot. archiwum

KATARZYNA KOPIEJCZYK
Absolwentka Wydziału Ekonomii Uniwersytetu w Białymstoku. Od 22 lat pracownik Białowieskiego Parku Narodowego. Początkowo pracownik Działu Finansowego, w latach 2013–2022 główny księgowy, obecnie zastępca dyrektora ds. administracyjnych, któremu podlegają zarówno pracownicy zaangażowani w zapewnienie turystom bezpieczeństwa i sprawnego udostępniania obiektów, jak i pracownicy czuwający nad bezpieczeństwem sieciowym i teleinformatycznym, niezbędnym do prowadzenia monitoringu i sprawnego funkcjonowania Białowieskiego Parku Narodowego.

CRN W sumie 6 tysięcy hektarów Parku znajduje się pod ścisłą ochroną. To znaczy, że wstęp dla osób postronnych jest tam zabroniony lub mocno ograniczony, na przykład tylko pod nadzorem autoryzowanego przewodnika. Jak radzicie sobie w tym zakresie z opanowaniem rzeszy turystów?
Monitorowanie ruchu turystów prowadzimy jeszcze przed ich pojawieniem się w Białowieży. Posiadamy dostępny przez internet system rezerwacji i sprzedaży biletów, poprzez który można wybrać konkretną godzinę wejścia do danego obiektu. Mamy poza tym specjalne kamery z fotokomórkami, które zliczają turystów w wybranych miejscach. Pozyskane z nich dane pozwalają nam obserwować natężenie ruchu i poziom zainteresowania poszczególnymi atrakcjami, na przykład ilu odwiedzających planuje wejście do muzeum, a ilu do rezerwatu pokazowego żubrów oraz ile miejsc parkingowych jest potrzebnych w terenie przy szlakach turystycznych czy edukacyjnych. Za pomocą takich samych kamer monitorujemy również dostęp do terenów niedopuszczonych do odwiedzania, będących pod ścisłą ochroną, na których obowiązuje reżim poruszania się. Nadzorem nad tym terenem zajmuje się Służba Parku wspierana przez Straż Parku. Jej zadaniem jest właśnie ograniczanie nielegalnych wejść na teren Parku i sprawowanie nadzoru nad przestrzeganiem prawa obowiązującego na jego obszarze.

CRN A jak wygląda ochrona przeciwpożarowa terenów leśnych?
Zadania z tym związane wykonywane są w ramach patroli pracowników terenowych. Korzystamy też z monitoringu wizyjnego, który pozwala zauważyć dym czy ogień w lesie. Korzystamy jednak tylko ze zwykłych kamer, które nie pozwalają dokładnie zlokalizować źródła pożaru. W tym zakresie współpracujemy z Lasami Państwowymi, które w razie potrzeby udostępniają nam dane ze swoich wież kontrolnych. W planach mamy wybudowanie własnego systemu wczesnego ostrzegania przeciwpożarowego wyposażonego w nowoczesne urządzenia do identyfikacji i lokalizacji źródeł zagrożeń. Mamy natomiast system monitoringu przeciwpożarowego w budynkach. Przez sieć mobilną i łącza telefoniczne jest on połączony z jednostką Państwowej Straży Pożarnej.

CRN Co jeszcze macie w planach na najbliższą przyszłość, jeśli chodzi o dziedzinę teleinformatyki?
Obecnie borykamy się chociażby z problemem braku odpowiednich łączy dostępowych do internetu. W części biurowej mamy sieć strukturalną, która korzysta z łącza po kablu miedzianym, który pozwala praktycznie na przepustowość rzędu 50 Mb. Takie są realia infrastrukturalne w miejscu, w którym się znajdujemy. Park jest na uboczu, na obrzeżach części zurbanizowanej. Ograniczenia finansowe, z którymi się borykamy, nie pozwalają nam na rozwój systemów w takiej skali, jak byśmy chcieli. Jesteśmy w trakcie przygotowania wniosku o dofinansowanie doprowadzenia światłowodu do budynku głównego i do części edukacyjnej. Chcielibyśmy też doprowadzić światłowód do rezerwatu pokazowego żubrów, gdzie są urządzenia multimedialne dla turystów. Wtedy być może można by było też udostępnić podgląd na żubry przez kamerę.

CRN W takiej sytuacji bazujecie zapewne na systemach obsługiwanych na własnej infrastrukturze?
Tak, mamy centrum danych z fizycznymi serwerami. Przy takich łączach jakimi obecnie dysponujemy, trudno myśleć o usługach chmurowych. Staramy się pozyskiwać środki zewnętrzne na dofinansowanie usprawnienia naszego działania, gdyż chcielibyśmy wraz z doprowadzeniem nowych łączy światłowodowych zmodernizować naszą całą infrastrukturę techniczną. Planujemy wymianę serwerów wraz z ich wirtualizacją, jak również wymianę switchy, firewalli, wdrożenie nowych zabezpieczeń.

CRN Jak liczny jest dział IT w BPN?
Zatrudniamy dwóch specjalistów – informatyków. Zajmują się większością prac związanych z obsługą, utrzymaniem, aktualizacją i dostępem do całego naszego środowiska informatycznego. Tam gdzie możemy, staramy się outsourcować zadania. Na przykład drukarki, a właściwie duże urządzenia wielofunkcyjne, dzierżawimy. Firma zewnętrzna obsługuje całe nasze środowisko druku w ramach abonamentu. W ramach zewnętrznej usługi odbywa się też obsługa firewalli. Liczymy na pozyskanie środków, które pozwolą nam w znaczący sposób ulepszyć posiadaną infrastrukturę teleinformatyczną i ułatwić jej obsługę.

Rozmawiał
Andrzej Gontarz

Puls branży IT

Istotne trendy rynkowe – produktowe, technologiczne, biznesowe – w oparciu o dane pochodzące z renomowanych agencji analitycznych, organizacji branżowych i globalnych mediów, dotyczące przede wszystkim Europy i Polski.

Ponad połowa firm płaci za chmurę

Liczba przedsiębiorstw kupujących usługi chmurowe wzrosła w Polsce o 27 pkt proc. wobec 2021 r., do 55,7 proc. w 2023 r. – podał GUS. Przy czym tak wysoki odsetek to w dużej mierze efekt korzystania z poczty elektronicznej, która pozostaje najpopularniejszą usługą chmurową w polskich firmach. Dopiero na drugim miejscu jest oprogramowanie biurowe. Mimo to, w porównaniu z czasem sprzed pandemii odsetek przedsiębiorstw, które płacą za usługi cloud, wzrósł kilkukrotnie. W 2019 r. z płatnych usług chmury obliczeniowej korzystało 17,5 proc. przedsiębiorstw, tj. o 6 pkt proc. więcej niż w 2018 r., w tym z poczty elektronicznej 12,9 proc. (o 5,2 p. proc. więcej wobec 2018 r.).

Przedsiębiorstwa kupujące usługi w chmurze (w % ogółu przedsiębiorstw)

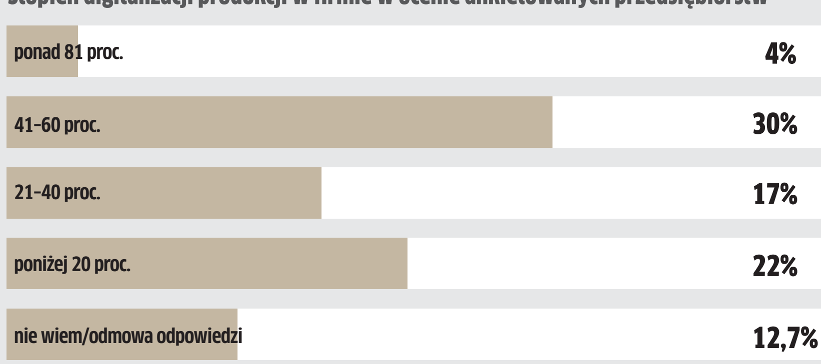
Rok	ogółem	w tym	
		e-mail	oprogramowanie biurowe
2021	28,7	22,6	18,3
2023	55,7	37,8	27,3

Źródło: GUS

Dłuższa droga do Przemysłu 4.0

Po przyspieszeniu cyfryzacji przemysłu w Polsce w ub.r., w tym roku niełatwa sytuacja gospodarcza zweryfikowała plany wielu firm, które musiały przesunąć w czasie kolejne etapy transformacji. Podawany przez Siemensa wskaźnik Digi Index, mierzący dojrzałość cyfrową średnich przedsiębiorstw produkcyjnych, spadł w 2023 r. do poziomu 1,8, a więc 0,6 niższego niż w 2022 r. (w skali od 1 do 4). Jako główne bariery w transformacji cyfrowej ankietowani mali i średni przedsiębiorcy wskazywali koszty (32 proc.) i nieumiejętność wykorzystania zgromadzonych danych (31 proc.). Wciąż dużych trudności przysparza im stosowanie procesów cyfrowych (wskaźnik 1,5), a najlepiej idzie zarządzanie danymi (3,0). Najbardziej zaawansowane w digitalizacji są firmy z branży motoryzacyjnej (2,0), a następnie produkcji maszyn oraz chemicznej i farmaceutycznej (w obu przypadkach 1,8). W tyle pozostaje sektor spożywczy (1,6). Słabiej wypadają małe firmy – digitalizację produkcji przeprowadziło mniej niż 20 proc. z nich. Z kolei dla dużych firm (ponad 250 pracowników), które zostały przeanalizowane po raz pierwszy, wskaźnik Digi Index jest wyraźnie wyższy i wynosi 2,7, co oznacza, że większość ankietowanych wykorzystuje cyfryzację w codziennej działalności operacyjnej. Tak dobry rezultat to efekt znacznie wyższych budżetów od MŚP i korzystania z międzynarodowych doświadczeń. Słabością dużych firm jest jednak obszar zastosowania procesów cyfrowych (2,1).

Stopień digitalizacji produkcji w firmie w ocenie ankietowanych przedsiębiorstw



Źródło: Siemens Polska, raport „Digi Index 2023”

„Zmęczenie CIO” ogranicza wydatki

Światowe wydatki na IT wzrosną w 2024 r. o 8 proc., do 5,1 bln dol. – prognozują analitycy Gartnera. Organizacje kładą obecnie nacisk w projektach na kontrolę kosztów, wydajność i automatyzację, ograniczając inicjatywy, które mogą przynieść zwrot dopiero po dłuższym czasie. Nowe wydatki opóźnia ponadto, jak to określono, zmęczenie CIO zmianami, co objawia się ich wahaniem przed inwestowaniem w nowe projekty i inicjatywy. Spowoduje to przesunięcie części nakładów na IT z 2023 r. na rok 2024, a tendencja ta ma się utrzymać w 2025 r. W 2024 r. segmenty oprogramowania i usług IT odnotują dwucyfrowy wzrost, głównie dzięki chmurze. Prognozuje się, że wydatki na usługi chmury publicznej zwiększą się w 2024 r. o 20,4 proc. Podobnie jak w 2023 r., źródłem wzrostu będzie połączenie podwyżek cen i zwiększonego wykorzystania usług. Cyberbezpieczeństwo napędza również dynamikę rynku oprogramowania. Natomiast w latach 2023 i 2024 r. jedynie bardzo niewielka część wydatków na IT będzie powiązana z generatywną AI. Jej wpływ w tym zakresie stanie się odczuwalny dopiero w 2025 r. Warto też odnotować, że w 2024 r. można w końcu liczyć na odbicie w segmencie urządzeń.

Prognoza światowych wydatków na IT w 2023 r. i 2024 r.

	Wydatki w 2023 r. (mld dol.)	Wzrost w 2023 r. (%)	Wydatki w 2024 r. (mld dol.)	Wzrost w 2024 r. (%)
Systemy centrum danych	237,703	4,7	260,221	9,5
Urządzenia	689,288	-10	722,472	4,8
Oprogramowanie	916,24	12,9	1 042,39	13,8
Usługi IT	1 401,04	7,3	1 547,35	10,4
Usługi komunikacyjne	1 449,29	1,8	1 497,35	3,3
W sumie	**4 693,56**	**3,5**	**5 069,77**	**8**

Źródło: Gartner

Rynek sieciówki nasyci się w 2024 r.

Europejski rynek infrastruktury sieciowej dla przedsiębiorstw (przełączniki ethernetowe, sieci WLAN i routery) wzrośnie w 2023 r. o 18,9 proc. rok do roku, osiągając wartość 14,3 mld dol. – wynika z danych IDC. Według analityków do skoku przychodów, jaki producenci odnotowali w 2022 r., przyczyniło się nadrabianie zaległości w dostawach. Ta dynamika utrzymała się w pierwszej połowie 2023 r., co doprowadziło do kolejnego silnego wzrostu wartości rynku w br. W 2024 r. zanosi się jednak na spadek na poziomie 7,6 proc. wobec 2023 r. w wyniku konieczności „przetrawienia” dostarczonych zaległych dostaw. Tym niemniej średnia roczna stopa wzrostu przychodów na rynku (CAGR) w okresie 2022–2027 powinna być dodatnia, ponieważ technologie sieciowe są kluczowe dla transformacji cyfrowej firm, a do tego odgrywają ważną rolę we wdrażaniu sztucznej inteligencji. W I poł. 2023 r. utrzymywał się silny wzrost obrotów na sprzedaży przełączników i korporacyjnych sieci WLAN. IDC spodziewa się, że wzrost na tych rynkach wyhamuje w drugiej połowie 2023 r., aby w 2024 r. osiągnąć wartości ujemne, głównie z powodu nadrobienia zaległości, a także ograniczeń w firmowych budżetach na infrastrukturę IT.

Źródło: IDC

Duży spadek inwestycji VC

Wartość inwestycji venture capital w Polsce w III kw. 2023 r. wyniosła 424 mln zł. W tym okresie 95 spółek pozyskało taką kwotę od 74 funduszy – wynika z raportu PFR Ventures i Inovo VC. Porównując sumę finansowania z trzech kwartałów w 2022 i 2023 r. nastąpił spadek o 54 proc. W tym czasie w regionie CEE wyniósł on 76 proc., a w Europie 49 proc. W III kw. br. odnotowano istotny spadek liczby tzw. rund zalążkowych, co ma związek z nałożeniem się globalnego dołka co do wycen i liczby transakcji z kończącym się w kraju programem POIR, który wkrótce zostanie zastąpiony przez FENG. Spadek przełożył się jednak na wzrost średniej wartości rund, która wyniosła 4,5 mln zł. Równolegle zwiększyła się liczba rund A i B. To oznacza, że do bardziej rozwiniętych spółek w końcu trafił kapitał, a w III kw. br. przeprowadzonych zostało 7 transakcji o wartości powyżej 10 mln zł. Towarzyszy temu wzrost znaczenia zagranicznych inwestycji polskich funduszy VC (po trzech kwartałach tego roku miały miejsce 44 takie rundy na łącznym poziomie 242 mln zł).

Wartość i liczba transakcji funduszy venture capital w Polsce w latach 2022 i 2023

	Wartość (mln zł)	Liczba
I kw. 2022 r.	1 172*	102
II kw. 2022 r.	877	92
III kw. 2022 r.	513	127
IV kw. 2022 r.	1 057	139
I kw. 2023 r.	444	127
II kw. 2023 r.	429	116
III kw. 2023 r.	424	95

**W tym 560 mln zł to megarundy - wyjątkowo wysokie transakcje*

Źródło: raport PFR Ventures i Inovo VC

Wacław Iszkowski
Autor w latach 1993–2016 był prezesem Polskiej Izby Informatyki i Telekomunikacji. Pracował też w firmach: Oracle, DEC Polska, 2SI, EDS Poland, TP Internet. Obecnie jest senior konsultantem przemysłu teleinformatycznego.

Obok cyberochrony, potrzebujemy ***cyber-kontrataków...***

O trendach w branży teleinformatycznej

Polska Izba Informatyki i Telekomunikacji opublikowała raport „Trendy w branży teleinformatycznej”. Pozwolę sobie wobec niego na kilka komentarzy, może nie tyle krytycznych, co raczej odmiennych od „poprawności biznesowej”, jaką wykazują się autorzy tego dokumentu.

Trzeba się zgodzić z autorami raportu, że cyfryzacja gospodarki jest warunkiem jej dalszego rozwoju, a ta w Polsce przebiegała w miarę dobrze. Niestety pandemia, wojna w Ukrainie, inflacja i brak „skoordynowanej strategii cyfryzacji gospodarki” podziałał hamująco na ten rozwój. Pesymistycznie brzmi prognoza spadku tegorocznych wydatków na teleinformatykę w Polsce o 0,5 proc.

Powinniśmy popierać hasło (tytuł) „Przemysł 4.0. Najwyższy czas na cyfryzację”, zwłaszcza że niestety mamy tutaj właśnie tylko świetne hasło, bez konkretów. Kolejnym trudnym tematem jest cyfryzacja administracji publicznej. Prawdą jest, że jakoś się informatyzuje – dała sobie radę z receptami, rejestracją szczepień, udostępnia usługi (np. do opłacania podatków) przez internet (o mObywatelu i ePUAP-ie już pisałem) itd. Jednak dalej wiele się musi jeszcze zmienić na zapleczu, gdzie wciąż obowiązuje papier z własnoręcznym podpisem.

Oczywiście kolejnym ważnym jest temat cyberbezpieczeństwa, czyli bezpieczeństwa systemów teleinformatycznych. Czytając po raz n-ty o problemach cyberbezpieczeństwa powraca mi uparcie myśl, że ten budowany tak mozolnie system wykrywania i gromadzenia informacji o zagrożeniach przypomina nieco linię Maginota – silnie ufortyfikowaną od frontu, a zdobytą przez Niemców od zaplecza. Tutaj tym zapleczem jest brak jakichkolwiek działań, aby było możliwe odcięcie sieci internetowej na określonym obszarze Polski lub Unii Europejskiej, tak aby mogła ona dalej funkcjonować, póki nie da się uporać z silnymi zagrożeniami zewnętrznymi, wtedy już bez bezpośredniego dostępu do naszych zasobów tej chwilowo autonomicznej sieci.

I jest jeszcze druga uparcie powracająca myśl, że obecnie filozofia cyberbezpieczeństwa opiera się tylko na obronie naszych zasobów teleinformatycznych. Nigdzie zaś nie ma informacji (a może są, ale tajne) o planach skutecznego wykrywania sprawców cyberataków oraz miejsca ich pobytu, a następnie o podejmowaniu działań odwetowych: złapania ich i osądzenia lub na dokonaniu wobec nich odwetowych cyberataków blokując lub niszcząc ich systemy. Oczywiście należy przy tym odróżnić sprawców prywatnych (przestępców) od państwowych (wojskowych), gdyż wtedy musi być inne postępowanie wymagające już podejmowania decyzji na wysokim szczeblu. Oczywiście te „złote” myśli powinny zaprzątać głowę politykom, a nie biznesowi.

A teraz ESG... Jak słyszę o konieczności raportowania z przestrzegania dobrych praktyk, to nie rozumiem o co chodzi, ale definitywnie jestem za nowym zielonym ładem. I szlag mnie trafia jak widzę ile drzew wokół jest ścinanych – w zasadzie każde drzewo powinno być już zapisane w systemie teleinformatycznym dla jego ochrony.

Nie bardzo za to podoba mi się hasło „demokratyzacja IT”, chyba że różnię się z autorami raportu w rozumieniu tego pojęcia. Mi się wydaje, że w informatyce

Rys. Adobe Stock

mamy wystarczająco demokratyczne zasady – każdy po kierunku informatycznym, mający odpowiednie kompetencje może znaleźć odpowiednią pracę (chyba, że ma jakieś ograniczenia lub wygórowane wymagania). Jak rozumiem, ma to być apel o zatrudnianie na tych stanowiskach osób z innym wykształceniem zawodowym lub biznesowym. Oczywiście w każdym przedsięwzięciu teleinformatycznym nie wszyscy w zespole muszą być teleinformatykami, ba – nawet nie powinno tak być, gdyż oprócz technicznych zadań informatycznych niezbędne jest rozumienie zakresu wiedzy przyszłych użytkowników oraz odpowiednia organizacja projektu. Powiedzmy więc, że demokratyzacja IT polega na dopraszaniu do prac IT osób mających specjalistyczną wiedzę na temat tego, co dany system ma przetwarzać, ale coraz bardziej z regulacji wynika konieczność dopuszczania do prac informatycznych tylko odpowiednio formalnie wyedukowanych oraz certyfikowanych specjalistów informatyków.

Ciekawy jest tytuł rozdziału „Sztuczna inteligencja. Obawa przed nieznanym". Rozumiem, że w takim raporcie należy używać skrótu AI, ale ja tutaj będę to nazywać systemem SI (w tym się też mieści słynny już „rewolucjonista" ChatGPT). W zasadzie trzeba się zgodzić z zaprezentowanymi przykładami możliwych zastosowań systemów SI, tym bardziej, że w tych opisach znajdujemy partykułę „może" nadającą im atrybut przypuszczenia czy osłabienia kategoryczności. Bowiem dopiero się przekonamy, które z tych zastosowań systemów SI przyniosły rzeczywisty pożytek i wzrost dochodów. Pośród tych zachwytów nad SI jednak niektóre z nich są nieco na wyrost. Na przykład NASK podaje, że „AI możemy powszechnie spotkać w motoryzacji, gdzie dba o proporcje spalanej mieszanki paliwa z powietrzem, czy w bardziej zaawansowanych modelach samochodów, gdzie automatycznie rozpoznaje znaki ograniczenia prędkości lub fakt, że samochód najeżdża na linię rozgraniczającą pasy ruchu bez włączonego kierunkowskazu". Akurat mam takie „mądre" auto i stwierdzam, że te „bajery" zostały oprogramowane przez inżynierów informatyków i mechaników bez używania metod SI, a wszelkie zmiany są do nich wprowadzane przez uaktualnienie oprogramowania pobranego z serwera fabrycznego. Nie przypisujmy wielu programom atrybutów systemów SI – one zostały zaprojektowane klasycznie przez utalentowanych inżynierów oprogramowania.

W uzupełnieniu tego rozdziału, TKP prezentuje problemy prawne związane z systemami SI, stwierdzając, że w chwili obecnej w UE nie ma aktu regulującego sztuczną inteligencję. A przecież takie akty są już przygotowywane i niebawem zostaną przyjęte, biorąc w karby systemy SI – szczególnie te wysokiego ryzyka, które mogą zagrozić osobom, społeczeństwom, komukolwiek.

Fundamentem cyfrowej transformacji, według autorów raportu, jest Big Data i analityka danych. W Polsce prognozy dotyczące rozwoju tych technik są korzystne (ponad 20 proc.). Oczywiście równocześnie musi mieć miejsce rozwój usług chmurowych, systemów SI oraz Internetu Rzeczy dostarczających tych danych w dużych ilościach. Dobrze, że autorzy raportu zwracają uwagę na ochronę gromadzonych danych, bo obawy użytkowników o ich bezpieczeństwo mogą hamować prognozowany rozwój.

Niestety nasz, środkowoeuropejski rynek IoT jest nieco zacofany w porównaniu do zachodniej Europy. Pewnym usprawiedliwieniem jest jeszcze ograniczony dostęp do 5G, mającego być podstawą komunikacji przez internet z sensorami. I jeszcze trzeba dodać Big Data oraz systemy SI. W raporcie tylko Samsung się pochwalił, że pomoże (sprzeda) zbudować inteligentne mieszkanie, dom, ulicę, całe miasto – wszystko będzie mogło być sterowane przez pilota, smartfona lub laptopa. Jakoś się tego obawiam, bo jak ktoś mi to zabierze, to zostanę całkiem odcięty od możliwości przetrwania w takim „pustym" środowisku. No cóż, postęp ma swoją cenę.

Zabawne, że „smart city", które zostało przetłumaczone na „inteligentne miasto", gdzie inteligencja polega na wykorzystywaniu zbieranych przez sensory danych do jego zarządzania, spotkało się ze sztuczną inteligencją. W raporcie podano, że w rankingu 183 inteligentnych miast są tylko dwa z Polski: Warszawa (62) oraz Wrocław (100). A obecnie, lekko licząc, można zebrać koło setki istotnych systemów teleinformatycznych, jakie są potrzebne miastu do jego funkcjonowania. Niestety przeszkodą jest brak wystarczających środków w samorządach bez finansowania z Unii. Niekiedy, ale już rzadziej, trzeba też pokonać zachowawcze poglądy urzędników na relacje z obywatelami, co utrudnia wdrożenie systemu SI korzystającego z inteligentnych IoT.

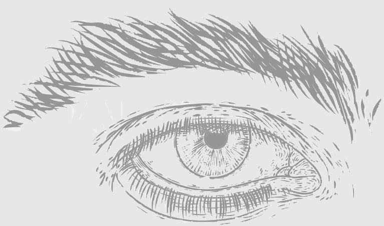
Chmura obliczeniowa to technika zdalnego przetwarzania danych przechowywanych w chmurze – istniejącym gdzieś w sieci, zewnętrznym zasobie pamięci masowej, będącej pod kontrolą innego podmiotu. Obecnie po dekadzie oferowania i korzystania z chmury, rozwiązanie to już stało się klasyczne, chociaż jeszcze jest wobec niego wiele zastrzeżeń. Stąd też podane w raporcie dane o wyłącznym korzystaniu z chmury przez tylko 17 proc. organizacji europejskich nie są zaskoczeniem. Jednak większość woli centra danych w swojej piwnicy. Dlatego też przed firmami oferującymi usługi w chmurach stoją jeszcze poważne wyzwania wyjaśniania potencjalnym klientom ich wątpliwości i zastrzeżenia. A ja jeszcze pamiętam przodka chmury obliczeniowej w postaci outsourcingu, gdzie nie tylko dane, ale również ich przetwarzanie było zlecane zewnętrznej firmie. I również wtedy było trudno przekonać organizacje, banki, firmy, aby ich „informatyka" była gdzieś poza zakładem.

Druga część raportu dotyczy telekomunikacji, a w zasadzie również teleinformatyki z podkreśleniem tele. Warto ją przeczytać. Całość jest dostępna pod adresem: www.piit.org.pl.

> Część zachwytów nad SI ***jest na wyrost.***

Wojciech Urbanek
zastępca redaktora naczelnego
CRN Polska

Europejskie muzeum *z filcowymi kapciami.*



Rys. Adobe Stock

Europa **jest liderem**

Europa jest jak autobus prowadzony przez niedowidzącego kierowcę, a nieświadomi pasażerowie krzyczą do niego: więcej gazu! Jak na razie udało się uniknąć katastrofy, ale to marne pocieszenie, zwłaszcza, że inne autobusy są już daleko z przodu.

Siedem lat temu, kiedy zaczynałem swoją pracę w CRN Polska, „popełniłem" felieton „Europa szuka nowej Nokii". Ubolewałem wówczas nad stanem europejskiej technologii, mając jednocześnie nadzieję, że uda się Europejczykom dołączyć do uciekających nam Amerykanów i Chińczyków. Niestety, jak się okazało, siedem lat to za mało, aby nie tylko dogonić uciekających liderów, ale chociażby nieco zniwelować dzielący nas do nich dystans. Co gorsza, nie widzę żadnych przesłanek, które pozwalałyby z nadzieją patrzeć na kolejne siedem lat. Europa coraz bardziej przypomina muzeum z filcowymi kapciami.

Być może trudno w to uwierzyć, ale w 2008 r. gospodarki Stanów Zjednoczonych i Unii Europejskiej były mniej więcej tej samej wielkości. Jednak sytuacja zaczęła się zmieniać na niekorzyść Europejczyków. Do 2022 r. wartość gospodarki USA wzrosła do 25 bln dol., podczas gdy UE i Wielka Brytania (łącznie) osiągnęły poziom 19,8 bln dol. Gospodarka amerykańska jest teraz o ponad 50 proc. większa niż obecnie unijna, a więc bez Wielkiej Brytanii. Te dane powinny być dla Europejczyków szokujące, stanowiąc obraz Starego Kontynentu, który pozostaje za światowymi liderami daleko w tyle, sektor po sektorze.

Niestety, nie inaczej jest w przypadku branży nowych technologii. Europejczycy korzystają z komputerów i smartfonów z logotypami producentów amerykańskich lub azjatyckich. To samo dotyczy centrów danych: w pierwszej siódemce największych firm technologicznych na świecie pod względem kapitalizacji rynkowej znajdują się wyłącznie koncerny amerykańskie. Do pierwszej dwudziestki załapali się tylko dwaj przedstawiciele Europy: AMSL oraz SAP.

Z czasem również Chińczycy czy Koreańczycy doczekali się własnych gigantów technologicznych, tymczasem europejskie, dobrze rokujące startupy są często połykane przez Amerykanów zanim przerodzą się w dojrzałe wizytówki Starego Kontynentu. Jak wszyscy pamiętamy, Skype'a kupił Microsoft, zaś DeepMind stał się własnością Google'a. Znamienny jest też sukces firmy Snowflake, obecnie z powodzeniem konkurującej z Oraclem. Jej założycielami są dwaj Francuzi oraz Polak, która to genialna trójka (piszę to bez cienia sarkazmu) postanowiła szukać swojego szczęścia nie w Paryżu czy Warszawie, lecz za oceanem, a konkretnie w San Mateo.

Jeszcze gorzej przedstawia się sytuacja na rynku półprzewodników. W 1990 r. udział Europy w ich światowej produkcji wynosił 44 proc. Obecnie jest to 9 proc., w porównaniu z 12 proc. należącymi do firm z USA. Jak powszechnie wiadomo Europa i Stany Zjednoczone chcą znacznie zwiększyć swoje zdolności w zakresie wytwarzania półprzewodników. W USA do 2025 r. ma być uruchomionych 14 nowych zakładów produkcyjnych, a w Europie i na Bliskim Wschodzie powstanie 10. Dla porównania w Chinach i na Tajwanie mają powstać... 43 fabryki.

Europa, a właściwie Niemcy, wciąż chlubi się swoimi autami. Audi, BMW, Mercedes, Porsche – to brzmi dumnie. Jednak to też niedługo może się zmienić. Niemcy najwyraźniej zakiwali się „grając w zielone". Eksperci są zgodni, że ich auta elektryczne nie będą miały szans w konkurencji nie tylko z Teslą, ale również chińskimi autami. Jak na razie takie marki jak BYD niewiele mówią Europejczykom, ale to tylko kwestia czasu, kiedy chińskie elektryczne samochody na dobre wjadą do Londynu, Berlina czy Amsterdamu.

Europa jest za to niekwestionowanym liderem w zakresie regulacji. Eurokraci cieszą się, że firmy na całym świecie też będą musiały przyjąć europejskie regulacje. Jednak złośliwcy uważają, że może lepiej byłoby przewodzić światu w tworzeniu bogactwa, niż go regulować... Czyżby mieli rację?


CATURIX
Wejdź na wyższy poziom
Gamingu: przedstawiamy
CATURIX
Dostępne u dystrybutora
Więcej informacji:
www.caturix.zone