Optymalizacja biznesu: bezpieczeństwo IT

Urszula Smoktunowicz

Potrzeby biznesowe kreują dziś projekty w każdym obszarze IT, również w obszarze security. W tej sytuacji dostawca musi dopasować się do trudnej roli zaufanego doradcy, który musi umieć zdiagnozować problem klienta i zaoferować mu rozwiązanie zapewniające jego usunięcie.

Na jakie ryzyka z powodu ataków mogą być lub są narażeni przedsiębiorcy i instytucje publiczne? Na przeróżne. – Hakerzy mogą próbować przejąć środki pieniężne organizacji (ostatni taki przypadek dotyczy Banku Narodowego Bangladeszu). W polskich warunkach ten scenariusz nie jest wcale aż tak nieprawdopodobny – zwłaszcza jeśli weźmiemy pod uwagę delikatne, ale jak najbardziej prawdopodobne zdarzenie, czyli możliwość działania osób wewnątrz organizacji klienta. Postępująca cyfryzacja samorządów niestety niesie też i takie zagrożenia (kilka lat temu agencja realizująca inwestycje w jednym z polskich miast utraciła kwotę kilku milionów zł poprzez świadomą podmianę numeru konta „w ostatniej chwili" – już po akceptacji przelewu przez zwierzchników na tzw. „dwie ręce") – mówi Mariusz Kochański, członek zarządu, dyrektor Działu Systemów Sieciowych, Veracomp.

W jego opinii kolejna kategoria ryzyk obejmuje zarówno te, związane z bezpośrednią utratą klientów na rzecz konkurencji (np. przez wyciek bazy stałych klientów), jak i z utratą ich zaufania do firmy, a w konsekwencji niechęć do dokonywania kolejnych transakcji (np. poprzez publiczny wyciek danych wrażliwych, m.in. numerów kart kredytowych, danych teleadresowych, numerów PESEL).

– Ryzyka związane z atakiem uniemożliwiającym prowadzenie normalnej działalności dotykają szczególnie firmy produkcyjne, ale też np. pizzerie korzystające z zamówień on-line czy systemy rekrutacji do szkół wyższych, średnich i przedszkoli. Dla firm produkcyjnych szczególnie istotne mogą być zdarzenia powodujące przestój linii produkcyjnej (np. przez wirusa atakującego system SCADA) czy magazynu (atak typu DDoS na sieć WLAN w magazynie korzystającym z przenośnych czytników kodów kreskowych jest w stanie uniemożliwić pracę) – dodaje Mariusz Kochański.

IT: REMEDIUM NA BOLĄCZKI BIZNESOWE

Czy przy takiej liczbie zagrożeń, nie jest przypadkiem tak, że obecnie nie tyle sprzedaje się rozwiązania IT, ile rozwiązuje problemy biznesowe za pomocą rozwiązań z obszaru security?

– W miarę wzrostu znaczenia i wartości informacji występujących w procesach biznesowych coraz częściej widzimy, że rozwiązania bezpieczeństwa stanowią odpowiedź na realne problemy związane z zapewnieniem ochrony danych i bezpieczeństwa aplikacji, urządzeń i systemów produkcyjnych klienta. Sprzedaż produktów z punktu widzenia dystrybutora staje coraz bardziej problematyczna, wymagając od klienta dużej wiedzy i świadomości dotyczącej podatności własnego systemu oraz wiedzy na temat możliwości zakupu konkretnego produktu, który taką podatność mógłby wyeliminować – zauważa Krzysztof Hałgas, Managing Director, Bakotech.

Jego zdaniem coraz większa ilość nowych, innowacyjnych rozwiązań, konieczność maksymalizacji efektywności biznesowej i szukania coraz bardziej zaawansowanych technicznie systemów ochrony skutkuje tym, że klienci nie znając ich kupują rozwiązania szablonowe, sprawdzone na rynku i dobrze znane, nie kierując się ich jakością bądź skutecznością, a własną wiedzą ograniczoną do znanych marek. – Często zakup takiego rozwiązania jest drogi (znana marka to duża marża producenta) oraz nieefektywny (kupujemy markę, którą znamy, a nie tę, która posiada narzędzia usuwające nasz problem). Coraz częściej jednak klienci wymagają od dostawców indywidualnego podejścia do ich problemów i wymuszają na rynku odwrócenie ról – od dostawcy sprzedającego konkretną markę po eksperta, który znajdzie problem, zdiagnozuje go i zaproponuje konkretne rozwiązanie. Takie podejście jest coraz bardziej widoczne na rynku i skutkuje tym, że coraz więcej dystrybutorów i dostawców skupia się na wybranych specjalizacjach, by móc oferować kompleksowe rozwiązania obejmujące dany obszar IT i rozwiązujące konkretne problemy biznesowe (np.: rozwiązania do ochrony danych w systemach klienta) – podkreśla Krzysztof Hałgas.

WYJŚĆ OD POTRZEBY BIZNESOWEJ

Agnieszka Szarek, Channel Account Manager, Fortinet, uważa, że to potrzeba biznesowa kreuje dziś projekty w obszarze security. Wynika to z różnorodności organizacji i specyfiki ich potrzeb. Dostosowujemy ofertę i rozwiązania do wyzwań i problemów, przed którymi staje klient, dlatego ważna jest kompletność i elastyczność rozwiązań – mówi.

Według Piotra Laskowskiego, dyrektora zarządzającego, ePrinus, to raczej zależy od typu rozwiązania i klienta. – Systemy typu DLP, AV (antywirus), filtrowanie sieci, itd., czyli proste „pudełkowe" rozwiązania, nadal sprzedaje się jako „zwykły soft". W przypadku bardziej zaawansowanych systemów, jak np. systemy: PIM, PAM, Policy Management, systemy kontroli dostępu" czy nawet systemy dwupoziomowego uwierzytelniania – faktycznie, interesuje się nimi „biznes". Coraz częściej to „biznes" generuje konkretne potrzeby i wskazuje działom IT i Security, jakie jest zapotrzebowanie, ale dotyczy to raczej firm większych i dojrzałych. Oczywiście nie możemy uogólniać. Każda firma działa w inny sposób. Jednak muszę przyznać, że od dłuższego czasu widzę postępujące zmiany i coraz większą świadomość w tym zakresie działów „biznesowych" i zarządów – ocenia.

Sprzedaż rozwiązań security może być realizowana na dwa sposoby. W tradycyjnym modelu sprzedaży relacyjnej koncentrujemy się na realizacji pojedynczej transakcji. Klient posiada potrzebę na konkretny produkt, którą zaspokajamy, realizując dostawę po ustalonej cenie. Możliwość maksymalizacji marży ogranicza się właściwie do dołączenia usług instalacyjnych czy rozszerzonej gwarancji.

Mariusz Kochański
członek zarządu, dyrektor Działu Systemów Sieciowych, Veracomp

Znacznie ciekawszy, ale i trudniejszy, jest model drugi bazujący na budowaniu długoterminowej relacji doradztwa. Jest ona oparta na wzajemnym zaufaniu, pozwala obu stronom na poszukiwanie modelu win-win, w którym większa marża sprzedawcy wcale nie musi oznaczać straty kupującego. Sprzedawca, pełniąc rolę doradcy, poszukuje w imieniu klienta optymalnego rozwiązania, które generuje konkretne dodatkowe przychody, chroni przed utratą aktywów czy poprawia produktywność organizacji klienta.

Doradztwo resellera może polegać na identyfikacji ryzyk (prawnych, operacyjnych, etc.) na podstawie dobrej znajomości modelu biznesowego klienta oraz szacowanie rzeczywistych strat i prawdopodobieństwa związanego z wystąpieniem konkretnego zdarzenia.

W opinii Chrisa Rottnera, Enterprise Account Executive'a i rzecznika prasowego w regionie CEE, AirWatch, każda zmiana w obszarze IT jest procesem, który powinien rozpocząć się od skutecznego zidentyfikowania i określenia problemów biznesowych. – Ten punkt wyjścia gwarantuje dobranie odpowiedniego rozwiązania bazujące na jednym lub kilku zintegrowa-

Arkadiusz Krawczyk
Country Manager
w Intel Security Poland

Po pierwsze na rynku jest bardzo dużo przeróżnych rozwiązań IT. Spojrzenie na nie jedynie przez pryzmat danych technicznych nie pozwala ich od siebie odróżnić. Ważniejsze jest to, co dzięki tym wszystkim parametrom poszczególne narzędzia mogą dać konkretnej firmie. Po drugie – decyzje budżetowe podejmuje zarząd, który niekoniecznie rozumie techniczne określenia, ale za to świetnie rozumie ich wpływ na działalność przedsiębiorstwa.

Pamiętajmy, że cyberatak to nie tylko kłopot dla działu IT, który musi usunąć zainfekowane pliki, uszczelnić system bezpieczeństwa czy ostrzec pracowników przed otwieraniem załączników z nieznanych źródeł. To przede wszystkim ogromny problem dla całego przedsiębiorstwa. Cyberprzestępcy nie dostają się do sieci firmowej tylko po to, żeby udowodnić sobie i innym, że potrafią to zrobić. Hakerzy włamują się przede wszystkim po to, aby wykraść dane przedsiębiorstwa. A wraz z danymi – np. danymi swoich klientów – firma traci zaufanie, reputację, kontrahentów. Cierpi na tym biznes. Dlatego dziś przedsiębiorcy nie szukają rozwiązań IT samych w sobie, ale właśnie remedium na problemy biznesowe; narzędzi, które pomogą im w prowadzeniu firmy i zdobywaniu zysków.

nych produktach. Jasne określenie zagrożeń, problemów i ryzyka dla codziennych operacji biznesowych musi być wstępem do każdego projektu security. Każdy sektor ma różne problemy, które muszą zostać zaadresowane, a co się z tym wiąże – będzie potrzebować różnych rozwiązań – zaznacza.

ROLA DOSTAWCY

A jaka jest w tym procesie rola dostawcy? Krzysztof Hałgas, Bakotech, zauważa, że wraz z pojawieniem się nowego podejścia nastąpiło niejako odwrócenie ról w procesie sprzedaży – stawiając dostawcę w trudnej roli zaufanego doradcy, który zamiast sprzedaży danego produktu, musi zdiagnozować problem i zaoferować klientowi rozwiązanie zapewniające jego usunięcie, a klienta w roli petenta, mogącego oprzeć się na wiedzy ekspertów, którzy w profesjonalny sposób pomogą w usunięciu problemu biznesowego.

Według Agnieszki Szarek, Fortinet, rolą dostawcy jest dostarczenie takiego rozwiązania, które skutecznie odpowie na konkretną potrzebę biznesową. – Dlatego ważne jest, by oferta dostawcy była możliwie kompleksowa, a projekty dokładnie skrojone pod danego klienta. Jako Fortinet jesteśmy w stanie odpowiedzieć w zasadzie na każdą potrzebę z obszaru cyberbezpieczeństwa – zapewnia.

W opinii Piotra Laskowskiego, ePrinus, dostawca musi występować jako konsultant i audytor, który uczciwie przeanalizuje i zaproponuje rozwiązanie, które sprosta oczekiwaniom/wymaganiom biznesu przy jednoczesnym podniesieniu poziomu bezpieczeństwa i nie utrudnianiu życia pracowników. – Ponadto jego zadaniem jest stworzenie odpowiedniej metodologii prowadzenia i wdrażania projektu. Coraz częściej widzę, że dostawca w tym zakresie nie musi być integratorem czy firmą wdrożeniową, gdyż te prace „fizyczne" może zlecić podwykonawcom specjalizującym się w tego typu zadaniach. Kluczowy jest jednak etap konsultacyjno/audytorsko/projektowy – podkreśla.

Zdaniem Chrisa Rottnera, AirWatch, rola dostawcy znacząco wzrasta i ewoluuje w kierunku zaufanego doradcy. – W dzisiejszych czasach zaufaniem klientów będą cieszyć się ci dostawcy, którzy nauczą się tłumaczyć język, którym biznes opisuje swoje problemy, na konkretne rozwiązania. Skuteczni przedstawiciele handlowi w obszarze IT muszą dotrzeć do biznesu, serca firm, i tym kanałem realizować sprzedaż opartą na pełnym zrozumieniu uwarunkowań procesowych swoich klientów. Dotychczasowy model sprzedaży poprzez działy informatyki może okazać się już niewystarczający – ocenia.

Arkadiusz Krawczyk, Country Manager w Intel Security Poland, uważa, że dostawca musi umieć spojrzeć na istniejącą sieć zabezpieczeń w firmie i powiedzieć, w jaki sposób zoptymalizować jej działanie, aby lepiej chroniła zasoby informatyczne przedsiębiorstwa. – Nie jest sztuką zalecenie wymiany wszystkich wdrożonych do

tej pory narzędzi na lepsze, wydajniejsze czy po prostu nowsze. Sztuką jest usprawnienie tego, co posiada firma, w taki sposób, aby przynieść jej wyraźne korzyści. To jest rola dostawcy, który w tym przypadku staje się nie sprzedawcą, a doradcą, rozumiejącym biznes i zdającym sobie sprawę z tego, że dla firmy istotna jest wydajność i oszczędności – zaznacza.

A W PRAKTYCE?

Jak przenieść taki model w praktyce na rozwiązania security?

Według Mariusza Kochańskiego, Veracomp, doradztwo w obszarze rozwiązań bezpieczeństwa można realizować w dwóch modelach: – Pierwszy to skupienie się tylko na zgodności działalności klienta z wymogami prawnymi regulującymi kwestię bezpieczeństwa IT, np. na ustawie o ochronie danych osobowych czy rozporządzeniach MSWiA. Takie wymogi stanowią dla klientów z branży samorządowej czy podmiotów prywatnych prowadzących działalność w modelu B2C konkretny zestaw wytycznych, których zlekceważyć nie można, ponieważ w przypadku niepomyślnego biegu wypadków (kontrola GIODO czy wyciek danych) grożą sankcje określone nie tylko prawem administracyjnym, ale również karnym. Doradztwo w tym obszarze będzie się zatem koncentrowało na wypracowaniu dla klienta optymalnego (koszty OPEX i CAPEX, czas wdrożenia, wymagania dla kadry) rozwiązania. Pole do inwencji dla resellera może dotyczyć np. optymalizacji kosztów CAPEX czy eliminacji wymogu posiadania wykwalifikowanej kadry administratorów (co oznacza wyższe koszty w liczbie etatów, wynagrodzeniach oraz szkoleniach).

Drugi model sprzedawania bezpieczeństwa polega na wyjściu poza obszar ograniczania ryzyk prawnych, w kierunku estymacji i ograniczania realnych ryzyk operacyjnych niosących prawdopodobieństwo wystąpienia zdarzenia niepożądanego – tłumaczy.

W jego ocenie osobną, szczególnie ważną, kategorią jest ryzyko utraty dobrej reputacji firmy w oczach klientów, banków finansujących, pracowników i kandydatów na pracowników, inwestorów. – Do tej kategorii można zaliczyć również utratę dobrej reputacji (tzw. powagi urzędu) przez władze administracyjne – atak przez haktywistów na stronę urzędu związany z podmianą treści spotkał już kilka lat temu KPRM. Takie ryzyka są zwykle dostrzegane przez zarządzających powierzonym im cudzym majątkiem – ta grupa osób charakteryzuje się bowiem znacznie większą awersją do ponoszenia wszelkich ryzyk operacyjnych – wylicza.

Jakie rozwiązania warto zastosować?

Mariusz Kochański, członek zarządu, dyrektor Działu Systemów Sieciowych, Veracomp: Oczywistą formą zabezpieczenia będzie na pewno ochrona stacji roboczych pracowników przy pomocy dobrego pakietu antywirusowego, np. F-Secure, oraz ochrona styku z Internetem przez urządzenie klasy UTM czy NGFW, jak Fortigate firmy Fortinet. Od razu warto zwrócić uwagę klienta na systemy WLAN – ich brak tworzy czasami złudne poczucie bezpieczeństwa administratora, tymczasem pracownicy pozbawieni własnego hot spota mogą dokonać niekontrolowanej instalacji własnego Access Pointa podłączonego do sieci wewnętrznej. Ponieważ klonowanie adresu MAC jest powszechną funkcjonalnością tych urządzeń, zabezpieczenie się przed takim scenariuszem poprzez listy ACL na przełączniku LAN nie jest skuteczne. Znacznie lepiej, gdy organizacja zbuduje własną sieć WLAN, wykorzystującą rozwiązania np. firm Aruba, Extreme Networks lub Fortinet, z osobnymi SSID dla gości i pracowników, wzmocnioną dobrze działającym systemem NAC (takimi mogą się pochwalić Aruba i Extreme Networks), a także sprawnym systemem rejestracji logów oraz filtracji niepożądanych usług i adresów.

Poczta elektroniczna staje się jednym z głównych potencjalnych mediów niosących zagrożenia – pliki PDF czy MS Office, linki czy skrypty zawarte w wiadomościach mogą być niebezpiecznie dla adresatów, dlatego warto zaproponować klientowi rozwiązanie zabezpieczające ten kanał komunikacji – ciekawe i skuteczne narzędzia proponuje Fortinet, Blue Coat czy Proofpoint.

Krzysztof Hałgas, Managing Director, Bakotech: Zapewnienie ciągłości i bezpieczeństwa działania procesów biznesowych jest kluczem do sukcesu każdej organizacji – rozwiązania takie jak monitorowanie wydajności i jakości działania usług sieciowych definiowanych według potrzeb użytkownika, uprawnień i zasad dostępu do krytycznych zasobów w organizacji, monitorowanie aktywności użytkowników, administratorów, ruchu sieciowego, aplikacji, ale także te chroniące dane użytkownika, jak ochrona antymalware'owa, antyspamowa, kontrola portów, treści danych, szyfrowanie kluczowych obszarów czy w końcu ochrona brzegowa sieci; wszystkie te elementy wydatnie podnoszą wydajność działania różnorakich procesów biznesowych każdej organizacji.

Chris Rottner, Enterprise Account Executive i rzecznik prasowy w regionie CEE, AirWatch: Konieczna dziś jest znajomość zagadnień zarządzania urządzeniami mobilnymi, mobilnością przedsiębiorstwa, dostępem do danych i aplikacji, kontroli tożsamości użytkowników, wirtualizacji stacji roboczych i ich cyklu życia. Te aspekty będą kluczowe w najbliższych latach dla wszystkich dostawców, którzy będą chcieli nadążyć za zmieniającymi się wymaganiami swoich klientów.

Arkadiusz Krawczyk, Country Manager w Intel Security Poland: Intel Security stawia na integrację, która leży u podstaw zalecanego do stosowania cyklu obrony przez zagrożeniami. Cykl ten łączy ochronę, wykrywanie i naprawę z centralnym zarządzaniem w czasie rzeczywistym w ramach elastycznego obiegu informacji. Takie podejście sprawia, że system bezpieczeństwa przyjmuje formę powtarzalnego cyklu, który nieustannie się doskonali.

Piotr Laskowski, dyrektor zarządzający, ePrinus: Systemy klasy PIM, PAM, Policy Management, kontrola dostępu (chodzi o kompleksowe systemy zapewniające wysoki poziom bezpieczeństwa i granulacji: kto, do czego i kiedy ma dostęp) oraz w mniejszym stopniu i w zależności od specyfiki klienta – również systemy uwierzytelniania.

Agnieszka Szarek, Channel Account Manager, Fortinet: Nie ma jednoznacznej odpowiedzi na to pytanie. Wszystko zależy od specyfiki klienta i jego potrzeb. Niemniej nasze produkty zostały zaprojektowane z nastawieniem na optymalizację w wielu aspektach, m. in. poprzez przejrzyste systemy zarządzania, analizy i raportowania, segmentację sieci czy wsparcie rozwiązań w chmurze.