Warszawa, 12 lutego 2020 r.

Informacja prasowa

**Atman rozszerza ofertę usług cyberbezpieczeństwa o rozwiązania Trend Micro**

**Atman jako pierwszy operator data center na polskim rynku wprowadził do swojego portfolio rozwiązanie Deep Security do ochrony serwerów. Technologia uznanej japońskiej firmy Trend Micro do tej pory wykorzystywana była przez duże firmy. Dzięki współpracy z Atmanem również organizacje mające niewielkie środowiska serwerowe będą mogły istotnie zwiększyć swój poziom ochrony przed atakami hakerskimi i złośliwym oprogramowaniem.**

Polski operator data center Atman zdecydował się ułatwić klientom dbanie o bezpieczeństwo środowisk serwerowych i włączył do oferty kompleksowe, a jednocześnie elastyczne rozwiązanie Deep Security. To efekt współpracy z firmą Trend Micro*,* światowym liderem w dziedzinie cyberbezpieczeństwa, mającym 30‑procentowy udział w rynku ochrony serwerów. Nowe rozwiązanie w portfolio warszawskiego operatora automatyzuje proces ochrony serwerów i znacząco upraszcza zarządzanie bezpieczeństwem firmowej infrastruktury bez względu na lokalizację (własna serwerownia, zewnętrzne data center, chmura obliczeniowa) i technologię (fizyczne, wirtualne, kontenery, a nawet serverless computing).

*Biorąc po uwagę przeznaczenie rozwiązania Deep Security, czyli ochronę środowisk serwerowych, bardzo nas cieszy pozyskanie lidera krajowego rynku data center jako partnera biznesowego w Polsce –* komentuje Krzysztof Gołda, Channel Manager w Trend Micro Poland. – *Głośne cyberataki z ostatnich lat dowodzą bezsprzecznie, że firmowe serwery muszą znajdować się w centrum uwagi osób tworzących strategie bezpieczeństwa organizacji. Każdy dział IT potrzebuje możliwie najszerszego zakresu narzędzi, które będą reagować automatycznie, broniąc zasoby IT firmy przed działaniami cyberprzestępców* – dodaje.

*Obserwując nieustającą ewolucję cyfrowych zagrożeń, nawiązanie współpracy z Trend Micro jest dla nas szczególnie istotne. Dzięki niej będziemy mogli wszechstronnie wspierać naszych klientów w chronieniu cennych zasobów IT. Narzędzia Deep Security świetnie uzupełniają dotychczasowe usługi Atmana z zakresu bezpieczeństwa, takie jak antyDDoS* – podkreśla Radosław Przybysz, kierownik produktu Deep Security w Atmanie. – ­*Firmy z pewnością docenią m.in. elastyczność rozwiązania Trend Micro. Dzięki jego modułowości każdy może zdecydować, czy chce korzystać ze wszystkich narzędzi Deep Security, czy tylko z wybranych, i może to zrobić niezależnie dla każdego serwera* – dodaje.

**Inteligentne bezpieczeństwo – także dla systemów już niewspieranych przez producenta**

Deep Security znacznie ogranicza ilość ręcznej pracy, jaką działy IT wykonują w zakresie cyberbezpieczeństwa, dzięki zautomatyzowaniu większości funkcji. Jest intuicyjne w instalacji i wygodne w zarządzaniu.

Na rozwiązanie składają się narzędzia służące do ochrony sieci i takie, które są skupione na ochronie systemów i aplikacji. Odrębny moduł Deep Security stanowi zabezpieczenie przed złośliwym oprogramowaniem. Obecnie nie wystarcza bowiem nawet najbardziej rozbudowany program antywirusowy. Różnorodność typów i stały przyrost tzw. malware’u wymaga odpowiedniego narzędzia, takiego jak Antymalware Trend Micro. Bazuje ono na wyjątkowo bogatej i stale aktualizowanej bazie złośliwego oprogramowania i jest zaliczane do najskuteczniejszych zabezpieczeń tego typu.

Szczególnym zainteresowaniem przedsiębiorstw cieszy się Virtual Patching – narzędzie opracowane z myślą o automatycznym zabezpieczeniu serwerów przed wykrytymi lub opublikowanymi podatnościami systemu operacyjnego serwera i zainstalowanymi na nim aplikacjami.

Ręczne dokonanie aktualizacji wymaga przerwy w pracy danego urządzenia, co w przypadku krytycznych serwerów może oznaczać nieplanowane przestoje w działalności operacyjnej firmy, a w rezultacie generować straty finansowe i wizerunkowe. Z kolei zwłoka w aktualizacji do czasu najbliższego okienka serwisowego to narażenie kluczowych systemów na cyberatak, a więc utratę lub wyciek wrażliwych danych.

*Świeża luka bezpieczeństwa jest bardzo szybko wykorzystywana do przeprowadzania prób cyberataków, dlatego dla utrzymania bezpieczeństwa systemu kluczowy jest minimalny czas reakcji od wypuszczenia przez producenta tzw. łaty, ang. patch, do jej instalacji. Innowacyjność i efektywność narzędzia Virtual Patching polega na automatycznym uruchomieniu w sieci wirtualnej łaty, która zabezpiecza tę lukę i chroni serwer do czasu zainstalowania oficjalnej aktualizacji* – opowiada Radosław Przybysz z Atmana. – *To jak gdyby nad nową szczeliną w naszym dachu automatycznie pojawiało się idealnie dopasowane pole siłowe. Taki mechanizm chroniłby nasz dom przez zalaniem, jednocześnie dając komfort odłożenia uszczelnienia dachu na dogodny dla nas moment.*

Firmy, które zdecydują się na narzędzie Virtual Patching, mogą mieć także pewność, że ich serwery są chronione przed atakami wykorzystującymi podatności nawet wtedy, gdy ich system operacyjny przestał (lub przestanie) być wspierany przez producenta. Świeży przykład to Windows Server 2008 i 2008 R2, które Microsoft zakończył wspierać 14 stycznia 2020 r.

*Wraz z wygaśnięciem wsparcia producenci przestają przygotowywać nowe łaty i wysyłać kolejne aktualizacje oprogramowania, mimo że nadal wykrywane są nowe podatności. Najlepszym sposobem uniknięcia narażenia na atak jest wcześniejsza migracja na inną, nowocześniejszą platformę sprzętową lub do chmury. Jeżeli jednak firma korzystająca z Windows Server 2008 zdecyduje się z jakichś przyczyn nadal pracować na tym systemie, powinna bezwzględnie wdrożyć zabezpieczenie* *typu Virtual Patching* – przestrzega Radosław Przybysz*. – Atman jest gotów w tym pomóc zarówno w przypadku maszyn kolokowanych lub wynajmowanych przez klientów w naszych centrach danych, jak i w przypadku serwerów utrzymywanych u innych operatów data center lub w firmowych serwerowniach on-premises –* zapewnia*.*

**Ochrona dla każdego**

W Polsce oferta Deep Security firmy Trend Micro była dotychczas ograniczona do organizacji utrzymujących i zabezpieczających wiele serwerów. Warszawski operator centrów danych Atman będzie świadczył tę usługę wszystkim firmom zainteresowanym profesjonalną cyberochroną środowiska serwerowego, niezależnie od jego wielkości i lokalizacji. Dzięki temu każda organizacja w naszym kraju będzie miała szansę skutecznie chronić swoje zasoby IT przed złośliwym oprogramowaniem i atakami hackerów. Jest to o tyle istotne, że małe firmy stanowiły aż 43 proc. organizacji dotkniętych naruszeniem bezpieczeństwa w 2019 r. i podobnego odsetka możemy się spodziewać w 2020 r.

*W małej firmie, w której wszystko spoczywa na barkach jednego specjalisty ds. IT,* *ręczne wykonywanie aktualizacji systemu może skutkować przerwą w działaniu firmy w najmniej odpowiednim momencie biznesowym. Z kolei odwlekanie aktualizacji choćby jednego serwera krytycznego naraża na atak całą firmową infrastrukturę informatyczną. Dzięki Deep Security tego typu procesy odbywają się automatycznie i nawet jedna osoba jest w stanie skutecznie i bez nieplanowanych przestojów przeciwdziałać zagrożeniom* – konkluduje Krzysztof Gołda z Trend Micro.

***ATM S.A.*** *jest notowanym na GPW liderem polskiego rynku centrów danych i ekspertem w zakresie bezpieczeństwa transmisji i przetwarzania danych. Pod marką* ***Atman*** *świadczy usługi kolokacji i dedykowanego hostingu oraz usługi w chmurze we własnych centrach danych o łącznej powierzchni 16 470 mkw. Wykorzystując swoje łącza zagraniczne i sieci światłowodowe w największych miastach Polski, Atman oferuje usługi szerokopasmowe, w tym dostęp do Internetu i transmisję danych. Więcej na* [*www.atman.pl*](http://www.atman.pl)*.*