MDR wreszcie w zasięgu sektora MŚP – Comodo CWatch MDR

Jeden z liderów wśród producentów rozwiązań do ochrony IT – firma Comodo, z dystrybutorem na terenie Polski firma It Partners security sp. z o.o. , zaprezentowała dziś nową usługę, która szczególnie powinna zwrócić uwagę sektora Małych i Średnich Przedsiębiorstw (MŚP) i instytucji użytku publicznego (tzw. „GOV"). Mamy bowiem do czynienia z MDR, czyli rozwiązaniem typowo korporacyjnym (ENTERPRISE), który bezkompromisowo jest w zasięgu finansowym i technologicznym dla MŚP i GOV. To z pewnością mały przełom na rynku. Jego nazwa to **Comodo CWatch MDR.**

Czym jest MDR? To skrót od: Managed Detection and Response, w wolnym tłumaczeniu oznaczający „Zarządzanie wykrywalnością i reakcją (na zagrożenia)". Jest to rozwiązanie z gatunku DiD (Defense in Depth) czyli „Ochrony w Głąb". Za wikipedią:

Obrona w głąb (ang. *defence in depth*) − taktyka projektowania zabezpieczeń dla systemów informatycznych. Polega ona na wprowadzeniu wielu, niezależnych warstw zabezpieczeń. Taka nadmiarowość znacząco podnosi poziom ochrony ograniczając skutki błędów i ataków.

Idea obrony w głąb jest zalecana w stosunku do systemów wymagających najwyższego zaufania. Amerykańska agencja bezpieczeństwa (NSA) określa ją jako „najlepszą praktykę", która bazuje na inteligentnym wykorzystaniu istniejących technik i technologii

MDR pozwala na stałe monitorowanie naszej sieci i elastyczne dobieranie odpowiedzi na zachodzące ataki i podatności. Do tej pory ze względu na koszta i zasobożerną naturę rozwiązania (chodzi głównie o czas, wiedzę i ludzi – potrzebnych do stałej analizy raportów generowanych przez systemy MDR), rozwiązania tego typu były przeznaczone dla bardzo dużych podmiotów, posiadających swoje sztaby i dywizje odpowiadające za ochronę IT w trybie rzeczywistym. Wraz z usługą Comodo CWatch MDR takie przeszkody dla mniejszych podmiotów są niwelowane. Dzięki długiej współpracy z dwoma czołowymi analitykami Enteprise Strategy Group: Tony'm Palmerem i Jack'iem Pollerem , Comodo udało się stworzyć rozwiązanie, które można w łatwy i szybki sposób wdrożyć na krytycznych elementach IT (m. in. komputerach, sieciach, stronach internetowych czy usługach chmurowych). Rdzeń obsługi systemu czyli Security Operations Center (SOC) jest w przypadku CWatch MDR traktowany jako usługa. Natomiast problem ogromnej ilości raportów rozwiązuje zaawansowany system automatyzacji SOAR (Security Orchestration Automation and Response), który sam zajmuje się powtarzającymi się i mniej ważnymi incydentami, skutecznie filtrując wszelkie false-positive (fałszywe alarmy). Dzięki temu administratorzy mogą skupić się wyłącznie na aktywnościach wyższego poziomu – takich jak aktywne wykrywanie luk i podatności, ustalanie priorytetów bezpieczeństwa, czy zarządzanie ryzykiem. W skrócie – administrator otrzymuje bardzo praktyczną platformę do stałego monitoringu swojej struktury IT oraz szybkiego reagowania na szeroką gamę zagrożeń, a także bardzo duży zakres informacji o aktualnym stanie swoich zabezpieczeń. To najbardziej zaawansowany sposób zabezpieczania swojej sieci. O tym jak ważne jest posiadanie systemów SOC i SIEM, można poczytać na blogu Media Recovery.

Jeśli jesteś zainteresowany takimi rozwiązaniem, możesz śmiało napisać do nas na adres karol.m@pancernik.it lub wybierając inną formę kontaktu na stronie http://pancernik.it

Żródła:

mediarecovery.pl
pancernik.it
paladion.net
wikipedia.pl
helpnetsecurity.com
comodo-polska.pl
zabezpieczenia.it