**Sophos Rapid Response – nowa usługa monitoringu i reagowania w trybie 24/7**



**Kraków, 17 listopada 2020** – Sophos udostępnił **nową usługę Rapid Response**. W ramach oferty zespół specjalistów producenta może szybko odpowiedzieć na cyberatak. Po zaangażowaniu **całodobowo** pomaga on w szybkim **identyfikowaniu** incydentów bezpieczeństwa, ich **neutralizacji**, eliminacji skutków i zapewnieniu przyszłej ochrony. To pierwsze tego typu rozwiązanie dostępne w ramach **stałej, jednorazowej opłaty**, uzależnionej od liczby użytkowników i serwerów w danej firmie. Z usługi mogą korzystać zarówno klienci firmy Sophos, jak i przedsiębiorstwa, które dopiero rozważają rozpoczęcie współpracy.

**Analiza i reakcja 24/7**

Usługa Rapid Response wdrażana jest na prośbę firmy, która zaobserwuje **podejrzaną sytuację** w swojej sieci, na okres **45 dni**. Po otrzymaniu zlecenia w ciągu kilku godzin inżynierowie Sophos uzyskują dostęp do krytycznej infrastruktury zaatakowanego przedsiębiorstwa aby **ocenić skalę oraz wpływ incydentu** na bezpieczeństwo danych. Pełna analiza źródeł ataku oraz narażonych obszarów odbywa się w ciągu 48 godzin, następnie **blokowany** jest dostęp przestępców do infrastruktury i oceniane straty. Firma otrzymuje także **szczegółowy** **raport** z informacjami o źródłach ataku, naruszonych danych oraz rekomendowanych środkach bezpieczeństwa. Przez kolejne tygodnie prowadzony jest **monitoring infrastruktury** klienta w celu weryfikacji, czy atak został prawidłowo zneutralizowany.

*– Atak może sparaliżować wszelką działalność, dlatego szczególnie istotna jest jego szybka neutralizacja. Zespół świadczący usługę Sophos Rapid Response blokuje prowadzone ataki, dzięki czemu firmy mogą szybciej wrócić do regularnej pracy. Usługa dopasowana jest do potrzeb przedsiębiorstw każdej wielkości: mniejszym zapewnia kompleksową ochronę, w większych może uzupełniać działania wewnętrznych działów IT i wspierać je w szybkim reagowaniu na incydenty –* mówi **Łukasz Formas, kierownik zespołu inżynierów w firmie Sophos**.

**W 3,5 godziny do sieci**

Eksperci firmy Sophos, odpowiedzialni za usługę Rapid Response, monitorują zagrożenia w cyberprzestrzeni **przez całą dobę**, siedem dni w tygodniu. Niedawno zidentyfikowali **nowe ataki** wykorzystujące złośliwe oprogramowanie **Ryuk**. Przestępcy zmienili dostawcę malware’u (z Emotet na Buer Loader) oraz wdrożyli **nowe narzędzia** do poruszania się w sieci. Do infekowania komputerów z systemem Windows wykorzystali **phishing** – wystarczyło im **3,5 godziny** od momentu otwarcia złośliwego załącznika przez jednego z pracowników, aby dostać się **do firmowej sieci**. W ciągu **jednego dnia** atakujący podejmowali już pierwsze próby uruchomienia ransomware’u.

*– W tym roku złośliwy kod ransomware był dla cyberprzestępców prawdziwą żyłą złota. Stanowił prawie 85% wszystkich ataków zidentyfikowanych przez analityków Sophos. Dzięki łatwemu dostępowi do narzędzi i oprogramowania na czarnym rynku przestępcy mogą w tydzień zarobić na okupach więcej,* *niż większość z nas przez całe życie. Ataki są często przeprowadzane nocą, gdy nie pracują zespoły IT w firmach –* wskazuje **Łukasz Formas.**

**Informacje o firmie**

Jako światowy lider zabezpieczeń nowej generacji, Sophos chroni przed najbardziej zaawansowanymi cyberzagrożeniami ponad 400 tys. firm różnej wielkości w ponad 150 krajach. Rozwiązania Sophos wykorzystują chmurę i sztuczną inteligencję, aby zabezpieczać urządzenia końcowe (laptopy, serwery i urządzenia mobilne) oraz sieci przed ewoluującymi metodami cyberprzestępców. Przy wsparciu SophosLabs – globalnego zespołu badającego zagrożenia – firma odpowiada na zagrożenia takie jak ransomware, malware, exploity, eksfiltracja danych, phishing czy indywidualnie dokonywane włamania przez cyberprzestępców. Platforma do zarządzania w chmurze Sophos Central integruje całe portfolio produktów nowej generacji Sophos w jeden system „zsynchronizowanej ochrony”, dostępny przez zestaw interfejsów API i obejmujący m.in. rozwiązanie Intercept X dla urządzeń końcowych oraz zaporę sieciową nowej generacji z rodziny XG Firewall. Firma oferuje również usługi łączące posiadaną technologię oraz aktywne przeciwdziałanie zagrożeniom (Managed Threat Response), szczególnie istotne w zmieniającym się dynamicznie świecie.

Sophos dąży do rozwijania i oferowania rozwiązań nowej generacji, aby zapewnić każdemu przedsiębiorstwu najwyższej klasy ochronę, zachowując jednocześnie prostotę zarządzania i umożliwiając redukcję kosztów. Wykorzystuje do tego m.in. zaawansowane funkcje infrastruktury chmurowej, uczenie maszynowe, interfejsy API, automatyzację i zarządzanie sposobami reagowania na zagrożenia. Firma sprzedaje swoje produkty i usługi za pośrednictwem globalnej sieci ponad 47 tys. partnerów i dostawców usług zarządzanych (MSP). Z innowacyjnych technologii Sophos mogą skorzystać także konsumenci indywidualni dzięki rodzinie rozwiązań Sophos Home. Firma ma siedzibę w Oksfordzie w Wielkiej Brytanii.

Więcej informacji można znaleźć na stronie www.sophos.com