**Co nas czeka w cyberbezpieczeństwie w 2021 roku? Przewidywania eksperta Sophos**



**Kraków, 26 listopada 2020** – W **2021 roku** cyberprzestępcy będą wykorzystywać na coraz szerszą skalę powszechnie znane, **wiarygodne** **narzędzia**, co ułatwi im poruszanie się po sieci **bez wykrycia**. Zmieni się też argumentacja związana z **żądaniem okupu** przez atakujących – nie tylko będą szyfrowali dane, ale też **wykradali wrażliwe informacje** i grozili ich upublicznieniem. W cyberbezpieczeństwie znajdzie też zastosowanie **podejście znane z epidemiologii** – eksperci będą tworzyli modele statystyczne, aby szacować realną liczbę zainfekowanych urządzeń.

**Dodatkowe wyłudzenia i początkujący hakerzy**

Coraz częściej cyberprzestępcy dzielą się między sobą narzędziami**.** Ich **łatwa dostępność na czarnym rynku** sprawia, że także w nadchodzącym roku stale będzie rosła aktywność **początkujących** hakerów. Będą oni wykorzystywali przede wszystkim oprogramowanie umożliwiające atakowanie **dużej liczby niewielkich celów**. Stale udoskonalane będą techniki i narzędzia, a gdy jedno zagrożenie zniknie, w jego miejsce szybko pojawiać się będzie kolejne. Zmieni się również **argumentacja związana z żądaniem okupu** – coraz częściej, poza szyfrowaniem danych, atakujący **wykradają** bowiem **wrażliwe informacje** i grożą ich publikacją, jeśli ich żądania nie zostaną spełnione.

**Nowe wykorzystanie botnetów**

W 2021 roku konieczne będzie przykładanie większej wagi do powszechnychzagrożeń, takich jak **botnety** (grupa urządzeń zainfekowanych złośliwym oprogramowaniem, których działanie może być zdalnie kontrolowane przez hakera). Celem takich ataków coraz częściej staje się nie tylko wykorzystywanie mocy obliczeniowej komputerów do kopania kryptowalut czy rozsyłanie spamu, ale też m.in. **zbieranie wrażliwych danych**, na przykład dotyczących geolokalizacji, które później są **sprzedawane na czarnym rynku**. Takie incydenty mogą wydawać się nieszkodliwe, jednak grożą otwarciem całego systemu na bardziej zaawansowane zagrożenia, takie jak ransomware.

**Legalne narzędzia „kryjówką” przestępców**

Duże wyzwanie dla cyberbezpieczeństwa w nadchodzącym roku stanowić będzie coraz częstsze stosowanie przez przestępców **powszechnie znanych, wiarygodnych narzędzi** i usług sieciowych o wysokiej reputacji. Umożliwia to im **poruszanie się po sieci bez wykrycia** aż do momentu uruchomienia złośliwego oprogramowania. Jednocześnie utrudnia analizę incydentów, gdyż takie działania nie są automatycznie oznaczane przez rozwiązania ochronne jako zagrożenie**.** W procesie reagowania na incydenty **wzrośnie** więc **rola specjalistów** **ds. cyberbezpieczeństwa**. Ich wiedza i doświadczenie będą ułatwiały wyłapywanie anomalii sugerujących podejrzaną aktywność.

**Rozwój „cyfrowej epidemiologii”**

Jaki procent wszystkich urządzeń jest zainfekowanych **niewykrytym złośliwym oprogramowaniem**? To kwestia równie trudna do oszacowania, jak procent populacji zarażonej koronawirusem. Podejście znane z epidemiologii może jednak w 2021 roku znaleźć zastosowanie także w cyberbezpieczeństwie. Eksperci będą tworzyli **modele statystyczne**,aby szacować ogólną liczbę infekcji urządzeń**.** Pozwoli toskuteczniej oceniać ryzyko powodzenia ataków, ustalać priorytety oraz rozwijać rozwiązania ochronne.

**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