Bezpieczeństwo

BYOD — prywatny sprzęt a bezpieczeństwo sieci firmowej

Paweł Wałuszko 03.04.2020

Model BYOD (pracy na własnym urządzeniu, ang. *Bring Your Own Device*) nigdy nie cieszył się w Polsce dużą popularnością. Choć jeszcze w 2012 r. media z entuzjazmem opisywały nową modę, trend ten do dziś nie doczekał się nawet własnej polskojęzycznej strony na Wikipedii. Z różnych powodów model BYOD się w Polsce nie przyjął, troszeczkę jak praca zdalna — miała być rewolucja, a jednak mało kto faktycznie na stałe pracuje z domu.

Prawdziwą rewolucję natomiast przyniosła pandemia koronawirusa. Wiele firm zostało zmuszonych do permanentnego zamknięcia swoich drzwi, a te, które chcą się utrzymać na rynku, jak najszybciej przestawiają część lub wszystkich swoich pracowników na model pracy zdalnej. (Nawiasem mówiąc, o tym, jak bezpiecznie pracować zdalnie, pisałem niedawno — zapraszam do lektury). Niestety, w przypadku cyberbezpieczeństwa i ochrony danych podczas pracy zdalnej, czas jest najgorszym doradcą.

W najlepszej sytuacji są firmy, które, gdy nadeszła konieczność pracy w domu, już posiadały procedury z nią związane, włącznie z przygotowaniem sprzętu dla każdego pracownika. Pracownik otrzymujący właściwie zabezpieczony komputer przynosi go do domu i poza podłączeniem urządzenia do Internetu, praktycznie nie ingeruje w ustawienia systemów zabezpieczających dane — tak wyglądałaby idealna sytuacja.

Niestety, nie każda firma jest tak adekwatnie przygotowana. Część przedsiębiorstw spotyka się z modelem pracy zdalnej po raz pierwszy i ulega presji czasu – projekty muszą iść do przodu, więc trzeba jak najszybciej umożliwić pracownikom wykonywanie swoich zadań na zapasowych laptopach z biura lub urządzeniach prywatnych. Oczywiście, cyberprzestępcy tylko na to czekają.

Pracownicy celem cyberprzestępców

Choć pracownicy korporacji od zawsze byli targetem dla cyberprzestępców, obecna pandemia i panika z nią związana oddaje jeszcze jedno narzędzie w ręce hakerów: element chaosu informacyjnego.

Źródła takie jak Check Point's Global Threat Index zauważają, że od stycznia b.r. zostały zarejestrowane ponad cztery tysiące nowych domen związanych z koronawirusem, 3% z nich zostało uznanych za złośliwe, a dodatkowe 5% za podejrzane (Źródło). W przypadku domen związanych z koronawirusem, prawdopodobieństwo, że będą złośliwe, jest statystycznie o 50% większe, niż w przypadku innych domen zarejestrowane w tym samym okresie, co świadczy o wykorzystywaniu chęci wiedzy o pandemii w celu szerzenia malware'u.

Warto zwrócić także uwagę na fakt, że w ostatnim miesiącu wzrosła również ilość ataków phishingowych, a w regionach objętych największą ilością zachorowań, takich jak Włochy, liczba ataków się podwoiła (Źródło). Sama Światowa Organizacja Zdrowia (World Health Organization) ze względu na dużą ilość dezinformacji i podszywającą się pod nią osób, została zmuszona do opublikowania informatora o bezpieczeństwie cybernetycznym w dobie pandemii.

(Zbyt) Szybkie przejście w tryb pracy zdalnej

W związku z zaistniałą sytuacją, działy IT stają przed równie dużym chaosem w zarządzaniu bezpieczeństwem danych. Przygotowanie nowych stacji roboczych i odpowiedniego back-endu jest pracochłonne. Sam koszt zakupu laptopów i odpowiedniego oprogramowania dla pracowników pracujących zdalnie może okazać się zaporowy dla wielu przedsiębiorstw, przez co zostaną one zmuszone do używania starszych, nieaktualizowanych systemów lub zezwolą na BYOD (dla przypomnienia: używanie prywatnych komputerów do celów służbowych).

Tutaj otwiera się furtka do wielu problemów. W przypadku firmy, która nie była przygotowana na BYOD, komputery prywatne są zupełnie poza kontrolą administratora i nikt nie ma gwarancji, że są one bezpieczne. **Paradoksalnie, w dobie ochrony przed koronawirusem, to pracodawca ma największą szansę na otrzymanie wirusa komputerowego w prezencie od pracownika.**

Jak nie stać się częścią statystyk

Warto pamiętać, że w cyberbezpieczeństwie, pośpiech jest najgorszym doradcą. Zbyt szybkie przejście na model pracy zdalnej może przynieść przedsiębiorstwom katastrofalne rezultaty. Jeden nieodpowiednio zabezpieczony komputer podłączony do sieci korporacyjnej, może przynieść wyciek haseł, własności intelektualnej lub spowodować ogromne straty danych z powodu ataku ransomware. (Najlepszym tego przykładem jest amerykańskie miasto Baltimore, które w 2019 r. w wyniku zaledwie jednego ataku ransomware szybko straciło ponad 18,2 mln dolarów.)

Równie groźny jest brak szybkiej reakcji na podejrzane zachowania w sieci. W przeciwieństwie do normalnego trybu pracy, w którym tylko służbowe komputery pozostają zalogowane do systemów korporacyjnych, osoby logujące się z zewnątrz naturalnie spowodują zmiany w ruchu i zachowaniu się sieci. Ten aspekt może spowodować brak zauważenia ataków przez osoby monitorujące bezpieczeństwo sieci.

Warto też zauważyć, że nawet brak wykrytych błędów przy monitorowaniu sieci wcale nie musi oznaczać, że sieć nie jest zaatakowana. W sytuacji gdy doszło do wycieku haseł, przestępca użyje prawidłowych danych do zalogowania się do systemów, więc tylko poprawny monitoring i korelacja metadanych (takich jak adresy IP i godziny zalogowań) pozwoli administratorowi zauważyć intruza.

Oprogramowanie

Na rynku istnieje wiele rozwiązań monitorujących sieć i zachowanie użytkowników. W Polsce bardzo popularne są oprogramowania z otwartym kodem źródłowym (ang. *open source*), np. Zabbix, Nagios lub OpenNMS. Dla tych, którzy preferują oprogramowanie komercyjne z dedykowanym supportem, istnieją też inne rozwiązania, takie jak AdRem NetCrunch (Polska), Paessler PRTG (Niemcy), lub Solarwinds NPM (USA).

Przy konfigurowaniu takich systemów warto zwrócić uwagę na monitorowanie zachowań skryptowych, tzn. takich, które najprawdopodobniej nie przydarzają się przeciętnemu użytkownikowi: kilka nieprawidłowych uwierzytelnień w ciągu jednej sekundy, identyczny czas dostępu (*access time)* do kilku folderów naraz, lub zalogowanie się z dwóch adresów IP jednocześnie.

Ponadto, używając powyższych systemów, przy odpowiedniej konfiguracji, można monitorować sieć pod względem wykrywania nienaturalnych zachowań użytkowników. Dla przykładu, nawet poprawne zalogowanie się z udziałem niestandardowego adresu IP może świadczyć o wycieku haseł. To samo można powiedzieć o poprawnym zalogowaniu się do sieci korporacyjnej poza standardowymi godzinami pracy – administrator powinien być poinformowany o każdym incydencie i manualnie zweryfikować kto i w jakim celu dokonał uwierzytelnienia.

Sztuczna inteligencja (Artificial Intelligence)

Biorąc pod uwagę fakt, że wybranie i wdrożenie odpowiedniego systemu do monitorowania sieci może być czasochłonne i duża część pracy związanej z weryfikowaniem obecnych w niej zdarzeń musi być wykonywana przez administratora manualnie, nic dziwnego, że najnowszym trendem są systemy wyposażone w sztuczną inteligencję. W porównaniu do systemów NPM (ang. *network performance monitor*), których głównym celem jest monitorowanie ruchu i urządzeń, rozwiązania oparte o AI monitorują zachowanie użytkownika i określają stopień zagrożenia tegoż zachowania w oparciu o multum metadanych generowanych przez użytkownika podczas codziennego korzystania z komputera i usług na sieci.

Największą zaletą rozwiązań opartych o sztuczną inteligencję jest ich bezobsługowość i zakres działania. W porównaniu do tradycyjnego monitorowania sieci, sztuczna inteligencja jest w stanie korelować dane z wielu źródeł jednocześnie, co pozwala na bardzo wczesne wykrycie niepożądanych zachowań. Ponadto, w przeciwieństwie do manualnej weryfikacji incydentów, sztuczna

inteligencja funkcjonuje całodobowo i może podjąć działania prewencyjne, gdy administrator jest poza biurem.

Reasumując

Przez obecną pandemię, praca zdalna i BYOD stały się realną częścią *modus operandi* wielu firm, które być może nie były na to przygotowane. Zważywszy na chaos informacyjny i zmiany w sposobie wykonywania pracy, cyberprzestępcy zwiększają swoje wysiłki, atakując przedsiębiorstwa w dobie transformacji — musimy być na to gotowi.

Najlepszą radą jest nieuleganie presji czasu i przygotowanie odpowiedniej infrastruktury *back-end*, jak i służbowych urządzeń, które mogą być wypożyczone pracownikom na czas pracy zdalnej. Biorąc pod uwagę ilość urządzeń zdalnych, które w zaistniałej sytuacji będą łączyły się z siecią korporacyjną, proaktywny monitoring sieci i zachowań jest niezbędny w zarządzaniu zmianami i wczesnym wykrywaniu anomalii w dobie zwiększonych ataków.

03.04.2020

Paweł Wałuszko

Business Development Manager i Ekspert ds. Bezpieczeństwa. Doświadczony menedżer w branży IT, który swoje doświadczenie zdobywał m.in. w Dolinie Krzemowej; entuzjasta oprogramowania open - source.

Koronawirus okazją dla cyberprzestępców. Na co uważać?