Problemy i wyzwania bezpieczeństwa IT

Z Mariuszem Kochańskim, członkiem zarządu i dyrektorem Działu Systemów Sieciowych w firmie Veracomp, rozmawia Marcin Marciniak.

Gdzie można mówić o największych problemach z bezpieczeństwem?
Zwykli użytkownicy są najczęściej dobrze chronieni, ryzyko ewentualnych strat jest tu z założenia ograniczone. Trudniejsza sytuacja jest tam, gdzie uprawnienia są z definicji wysokie – u użytkowników uprzywilejowanych. Problem nie wynika z niskiej świadomości lub złej woli tych osób, ale stąd, że jeśli potencjalnemu włamywaczowi uda się podszyć pod takiego użytkownika, to zyska dużo większe możliwości działania. Mówiąc wprost, bardziej opłaca się przechwycić konto administratora niż prezesa firmy, bo prezes ma uprawnienia tylko do swojego konta, a administrator do wszystkich.

Jakie widzi Pan sposoby na obniżenie tego ryzyka?
Po pierwsze, zadbanie o to, by uwierzytelnianie tych osób było silne i trudne do podrobienia. Jeśli elementem uwierzytelnienia jest hasło, to niech będzie odpowiednio silne i często zmieniane. Po drugie, monitoring aktywności z takich kont, by potencjalnie niebezpieczne zdarzenia udało się wykryć na wczesnym etapie.

Częste zmiany mocnych haseł to brzmi jak porada z ubiegłego wieku. Czy zapominamy o dwuskładnikowym uwierzytelnieniu?
Jeśli przyjąć czysto statystyczne badanie, w którym sprawdzamy, do ilu urządzeń i systemów administrator ciągle się loguje w modelu login/statyczne hasło, to ta pozornie oczywista porada niestety nadal ma sens. Duże systemy dysponują możliwością integracji z dwuskładnikowym uwierzytelnieniem, ale część infrastruktury informatycznej nadal tego nie ma. Ten obszar wymaga uwagi, bo nawet przy najwyższych kwalifikacjach administrator jest tylko człowiekiem. Nie można oczekiwać, że będzie bezbłędnie, samodzielnie i regularnie wymyślał i zmieniał silne hasła.

Wspomniał Pan o monitoringu jako o swoistym radarze wczesnego ostrzegania.
Jest niezbędny, by wykryć na wczesnym etapie potencjalnie niebezpieczne zachowania, zwłaszcza z kont uprzywilejowanych. Do tych zachowań należą: rejestracja sesji, kolekcjonowanie logów z systemów SIEM i szybkie wnioskowanie, że zestaw pewnych aktywności może być związany z atakiem z konta uprzywilejowanego bez wiedzy prawowitego użytkownika. Trzeba ten atak możliwie wcześnie wykryć i podjąć odpowiednie działania.

Wtedy należy dać odpowiedź na zagrożenie. Dlaczego to jest takie trudne?
Wielowektorowość ataków i ich rozciągnięcie w czasie są poważnym wyzwaniem, jak się bronić. Obecnie producenci rozwiązań stawiają bardziej prowokacyjne pytania związane ze świadomością o ataku. Ile czasu upłynęło od ataku do momentu, w którym się o nim dowiedziałeś? Jak określić szkody, które poniosłeś? Ten czas musi być krótki, a ocena sprawna i precyzyjna.

Mamy zatem do czynienia z wyścigiem pocisku i pancerza.
Tak, z jednej strony dane naprawdę poufne należy trzymać w miarę możliwości zaszyfrowane, w infrastrukturze z wielowarstwowym zabezpieczeniem. Na nowe trendy zagrożeń trzeba także odpowiadać za pomocą odpowiedniej architektury systemów bezpieczeństwa, nie poprzestawać na firewallach, IPS-ach i zabezpieczeniach stacji roboczych. Trzeba wspomóc administratorów w detekcji ataków wolnozmiennych i monitorować także aktywność kont uprzywilejowanych, by zaradzić 80% potencjalnych ataków. Oczywiście, jednocześnie trzeba budować świadomość użytkowników, bo infrastruktura zawsze będzie gdzieś miała potencjalnie słabszy punkt.

Gdzie jest ten słaby punkt?
Wyzwaniem jest bezpieczeństwo infrastruktury sieciowej – w łączach kablowych to było proste, ale migracja do Wi-Fi przynosi kwestie związane z uwierzytelnieniem, podsłuchem, atakami przez celowe rozłączanie sesji bezprzewodowych. Przejęcie firmy Aruba przez HP jest znamiennym sygnałem, że w dziedzinie infrastruktury sieciowej WLAN klasy enterprise będzie następowało coraz silniejsze współzawodnictwo. Nadal istotne będą zagadnienia związane z bezpieczeństwem sieci bezprzewodowych, integracją systemów NAC z systemami radiowymi, pojawi się także popyt na systemy heterogeniczne. Na razie nie jest to takie proste, bo organizacje dopiero budują swoje doświadczenia w obszarze BYOD.

Jak w tym labiryncie ocenia Pan obecność prywatnych urządzeń?
To ciekawa kwestia, szczególnie w organizacjach, które dotąd były przyzwyczajone do ścisłych procedur. One były skuteczne w modelu, w którym sprzęt jest pod kontrolą działu IT i pracownicy spędzają cały czas w biurze. Ale dziś przestaje to być takie pewne. Nie zadeklarujemy, że smartfony są zakazane albo że nie wolno logować się w kawiarni. Największe zmiany przychodzą od strony kadry zarządzającej, która niejako z definicji jest odpowiedzialna za kulturę innowacji w organizacji. Zwykle to oni są ambasadorem zmian w takich obszarach, jak: praca grupowa, mobilność czy BYOD. Niestety, z tego powodu są również dobrym celem ataku. Jeden z producentów pokazał nam genialny w swojej prostocie atak polegający na uruchomieniu hotspotu o nazwie kafejki z cyfrą 2 i podsłuchiwaniu przechodzącego przez niego ruchu. Dziewięciu na dziesięciu „zwykłych" użytkowników uznaje taki punkt dostępu za bezpieczny.

Czy nadal problemem jest człowiek?
Niezbędne będą procedury i szkolenia, a także zamknięcie pętli sprzężenia, by całość nie była tylko jednorazowym działaniem. Pracownicy biurowi, którzy mają dostęp do zasobów IT, nawet do tych najprostszych, takich jak poczta elektroniczna, muszą mieć świadomość potencjalnego zagrożenia atakiem, zwłaszcza kradzieży ich tożsamości. Przez ostatnich 25 lat udało się przyzwyczaić ludzi, by przed wyjściem z firmy zamykali okna i aktywowali system alarmowy. Świadomość fizycznego włamania i kradzieży jest więc duża. Teraz trzeba podobną świadomość obrony stworzyć dla bezpieczeństwa IT, to wymaga szkoleń, zaangażowania innych działów firmy, np. HR. BYOD i ataki APT powodują, że działy IT będą spędzać więcej czasu na analizie modeli zachowań użytkowników i klientów, aby do nich dostosować politykę bezpieczeństwa. Dzisiaj głównym motywatorem ich wyborów jest dostępność i łatwość użytkowania narzędzia, a nie jego bezpieczeństwo. Musimy wspólnie, jako cała branża, popracować, aby to zmienić.

Czy w przyszłości jednym z wyróżników nie będzie wygoda, ale bezpieczeństwo?
Kiedyś Lukas Bank zbudował bazę rzędu miliona klientów dzięki nowemu modelowi bankowości. Zamiast tradycyjnych okienek – placówka z kawą, gdzie klient siada na równej pozycji z doradcą. To był autentyczny wyróżnik, także w kampanii reklamowej. Potem internet doprowadził do zmiany modeli biznesowych w kilku sektorach, stając się nowym wyznacznikiem dla wielu graczy. Wyciągając wnioski z przypadków takich jak Sony czy Target, można postawić hipotezę, że w przyszłości w branżach B2C takim wyróżnikiem będzie bezpieczeństwo – e-usługa dla klienta, która nie będzie najtańsza, ale bezpieczniejsza niż u konkurencji. Bezpieczeństwo będzie kluczem do zdobycia i utrzymania klienta.

Dziękuję za rozmowę.

veracomp