Reagowanie na zdarzenie

W sytuacji, gdy nie został jeszcze powołany zespół reagowania na incydent, nie zostały opracowane plany, brak jest narzędzi i list kontrolnych, priorytetem powinno być powstrzymanie incydentu bez niszczenia dowodów. Zazwyczaj jest to wykonywane przez kombinację zamykania lub poddania kwarantannie systemów, zmiany haseł, odwoływanie dostępu i blokowanie połączeń sieciowych. Jednocześnie zalecane jest skontaktowanie się z firmami zajmującymi się reagowaniem na incydenty i uzyskanie od nich informacji potrzebnych do lepszego przygotowania się na incydenty w przyszłości.

Co należy zrobić w przypadku odkrycia czegoś, co wygląda jak prawdziwy atak? Odpowiedź na takie pytanie w dużej mierze zależy od działań podjętych przez osobę atakującą oraz od tego, jak wygląda przyjęty model zagrożenia, aczkolwiek istnieje kilka wskazówek, które mogą być pomocne.

W pierwszym etapie należy zmobilizować przynajmniej część zespołu tak, aby dokonać oceny stanu zaatakowanego systemu. Nie ma sensu angażowanie 30 osób z powodu infekcji złośliwym oprogramowaniem, która po kilku minutach dochodzenia wydaje się całkowicie opanowana. Tak jak łatwo jest o przesadną reakcję, tak samo łatwo o reakcję zbyt słabą. W takim przypadku mogą być pomocne pewne wstępnie zdefiniowane poziomy istotności i wytyczne dotyczące reakcji dla każdego z tych poziomów.

Następnie należy rozpocząć realizację opracowanych planów, starając się przewidzieć najbardziej prawdopodobne cele osoby atakującej, opierając się na kill chains lub attack chains.

Cyber Kill Chains

Jak wspomniano już na początku tego rozdziału, jednym z najpopularniejszych obecnie łańcuchów jest Lockheed-Martin Cyber Kill Chain. Zgodnie z tym modelem można wyróżnić następujące fazy zagrożenia:

Rozpoznanie
: Przez osobę atakującą przeprowadzane są badania, mające na celu określenie, gdzie można się włamać i jakie podatności mogą być w tym pomocne. Działania takie mogą obejmować wszystko, od wyszukiwania w Google, grzebania w śmieciach, inżynierię społeczną, po skanowanie portów sieciowych.

Uzbrajanie
: W tym etapie tworzone jest złośliwe oprogramowanie w celu wykorzystania znalezionych luk. Bardziej zaawansowani atakujący mogą napisać coś niestandardowego, aczkolwiek w przypadku mniej zaawansowanych ataków może być użyte standardowe oprogramowanie znalezione w internecie.

Dostarczanie złośliwego kodu
: Ofiara jest zmuszana przez osobę atakującą do wykonania złośliwego oprogramowania, najczęściej przez atak sieciowy, wysłanie e-maila lub w inny sposób.

Eksploitacja
: Szkodliwe oprogramowanie zaczyna działać i następnie uzyskiwany jest nieautoryzowany dostęp.

Instalacja
: Złośliwe oprogramowanie jest umacniane przez instalację utrudniającą znalezienie i usunięcie tego oprogramowania, co jest zgodne z intencjami osoby atakującej. Często pierwszy kawałek złośliwego oprogramowania jest wykorzystywany do pobrania i instalacji drugiego elementu złośliwego oprogramowania. W niektórych przypadkach to trwałe złośliwe oprogramowanie jest lepiej obsługiwane i aktualizowane niż legalne programy użytkownika!

Command and control
: W wyniku działania złośliwego oprogramowania tworzony jest pewnego rodzaju kanał komunikacyjny, który umożliwia osobie atakującej zdalną kontrolę nad nim: zdalna powłoka, wychodzące połączenie internetowe, a nawet odczyt poleceń z usługi przechowywania plików w chmurze. W tym momencie dostęp do systemów może być sprzedany na czarnym rynku w dobrej cenie komuś, kto takiego dostępu potrzebuje.

Działania na „przejętym" celu
: Osoba atakująca, która może nawet nie jest pierwotną osobą atakującą, jest w stanie zrobić wszystko, co chce: ukraść dane, zniszczyć witryny, zaatakować klientów, wyłudzać pieniądze itp.

Inne popularne łańcuchy, takie jak MITER ATT&CK zawierają nieco inne etapy. Niezależnie od tego, który z łańcuchów jest wykorzystywany, dobrym pomysłem jest zapoznanie się z co najmniej jednym z nich, tak aby mieć pojęcie o tym, co napastnik mógł już zrobić i co może zrobić dalej.

Pętla OODA (Obserwacja-Orientacja-Decyzja-Akcja)

Kolejnym etapem po sporządzeniu planu, określeniu postępów i planów osoby atakującej jest reakcja. Popularną koncepcją reagowania na incydenty jest pętla OODA: obserwuj, orientuj, decyduj i działaj:

1. W fazie *obserwacji* należy zebrać informacje z systemów, takie jak dzienniki dostawcy usług w chmurze, zapór sieciowych, systemu operacyjnego oraz mierniki i inne lokalizacje pomocne w znalezieniu nietypowych zachowań, które mogą wskazywać na aktywność osoby atakującej.
2. W fazie *orientacji* należy zrozumieć, co się dzieje i co może się stać dalej. Może to obejmować zarówno wewnętrzną wiedzę o tym, gdzie znajdują się najważniejsze zasoby, jak i zewnętrzne informacje o zagrożeniach dotyczące tego, kto może być odpowiedzialny za atak i dlaczego. Nie wszystkie informacje o zagrożeniach są płatne. Na przykład US-CERT (*https://www.us-cert.gov/*) regularnie publikuje