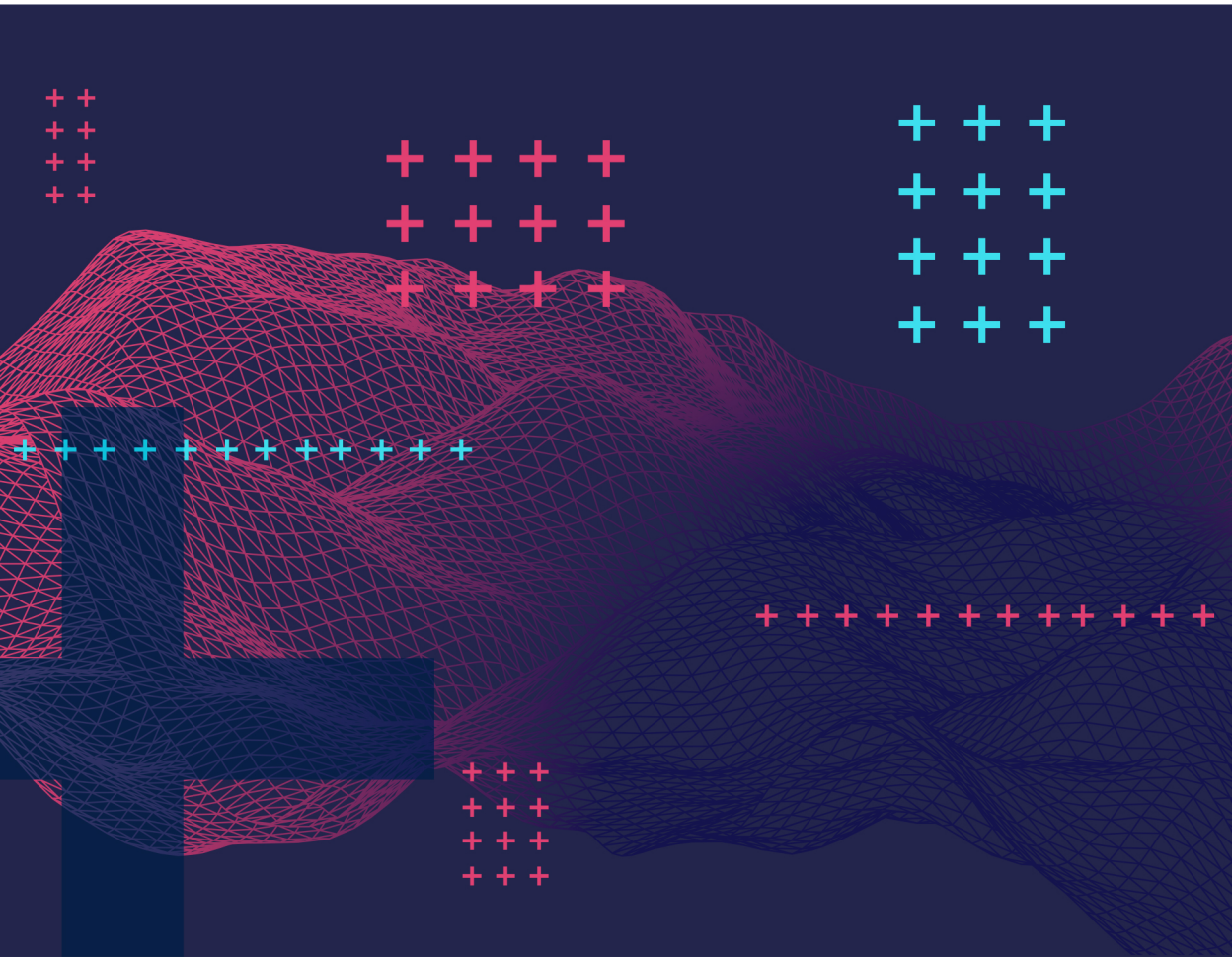
WYKRYWANIE, REAGOWANIE I ODZYSKIWANIE

po incydentach bezpieczeństwa



PWNING_WEEK 2021

PWN

ROZDZIAŁ 7

Wykrywanie, reagowanie i odzyskiwanie po incydentach bezpieczeństwa

W poprzednich rozdziałach zostały omówione zasoby w chmurze oraz ich rozsądne zabezpieczanie. Wszystko to wygląda dobrze, prawda?

W momencie gdy przeczyta się dwie trzecie powieści kryminalnej, a tajemnica wydaje się już rozwiązana, pozostaje świadomość, że historia się jeszcze nie skończyła. Prawdopodobnie nie jest wielką niespodzianką, ponieważ w tej książce są jeszcze strony do przeczytania, że konieczne jest jeszcze omówienie bezpieczeństwa chmury.

Wszystkie poprzednie rozdziały dotyczyły identyfikacji zasobów oraz ich ochrony. Niestety nie zawsze zapewnia to odniesienie sukcesu. W rzeczywistości w niektórych organizacjach i branżach drobne incydenty związane z bezpieczeństwem zdarzają się rutynowo! W pewnym momencie praktycznie na pewno pojawią się atakujący, którzy spróbują, czasem z powodzeniem, uzyskać nieautoryzowany dostęp do zasobów. Cała sztuka polega na tym, aby wykryć ich tak szybko, jak jest to tylko możliwe, zablokować im dostęp oraz wykonać wszelkie niezbędne kontrole ewentualnych szkód. Do przeprowadzenia tego bardzo pomocne jest zrozumienie, jak na ogół postępują osoby atakujące oraz w jaki sposób ataki są realizowane.

W ciągu ostatnich kilku lat zaobserwowano wiele głośnych włamań. Tym, co pozwala na odróżnienie groźnych ataków od tych naprawdę groźnych (nie ma niegroźnych!!!), jest czas, jaki upłynął do momentu wykrycia, co się wydarzyło oraz jaka była reakcja ofiary. Na podstawie badań 477 firm (*https://ibm.co/2GhfKMR*) wykazano, że średni czas na wykrycie naruszenia wynosił 197 dni, a firmy, które wykryły naruszenie w czasie krótszym niż 100 dni, zaoszczędziły dzięki temu ponad 1 milion USD w porównaniu z firmami, którym zajęło to ponad 100 dni. Mając to na uwadze, w książce została przedstawiona analiza możliwych rozwiązań, mających na celu wykrycie problemów oraz reagowanie na nie, zanim staną się katastrofą.

Kill Chains

Istnieje kilka rodzajów *kill chains* (wzorowanych na wojnie fizycznej), które zawierają próbę opisu postępowania osoby atakującej. W momencie pisania tej książki najpopularniejsze z nich to Lockheed Martin Cyber Kill Chain (*https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html*) oraz MITER ATT&CK framework (*https://attack.mitre.org/*) (wymawiane jak „atak"), aczkolwiek wiele innych zostało udokumentowanych w pracy CIA *The Unified Kill Chain* (*https://www.csacademy.nl/images/scripties/2018/Paul_Pols_-_The_Unified_Kill_Chain_1.pdf*) autorstwa Paula Polsa.

Owe *kill chains* zawierają opis typowych kroków osoby atakującej, takich jak rozpoznanie, uzbrojenie, dostawa, eksploitacja, instalacja, kontrola oraz działania na celach. Zalecane jest, aby zespół do spraw reagowania na incydenty przeczytał i zrozumiał przynajmniej jeden z tych *kill chains*, ponieważ zrozumienie kroków, które mogą podjąć atakujący, może być pomocne w reakcji na realny atak. Przykład został omówiony w dalszej części tego rozdziału.

Różnice w stosunku do tradycyjnego IT

Jako punkt odniesienia ponownie został wykorzystany schemat modelu współodpowiedzialności z rozdziału 1 (rysunek 1.8).

W tradycyjnym środowisku konieczne było zajmowanie się tym, co działo się na każdym z poziomów. W przypadku dostawców usług w chmurze pozytywne jest to, że podobnie jak w przypadku innych kontroli, wykrywanie włamań i reagowanie na nie jest zadaniem dostawcy w obszarach, za które są odpowiedzialni. W przypadku naruszenia u usługodawcy, użytkownik powinien zostać o tym powiadomiony i następnie konieczne może być wykonanie działań związanych z reagowaniem i odzyskiwaniem w zależności od wykorzystywanych usług. Jednak w zdecydowanej większości przypadków wszystkie działania związane z wykrywaniem, reagowaniem i odzyskiwaniem dotyczą obszarów oznaczonych jako „odpowiedzialność klienta".

W większości przypadków nie ma możliwości przeglądania dzienników dotyczących poziomów, za które odpowiedzialność ponosi dostawca, aczkolwiek czasami możliwe jest zaobserwowanie działań podjętych przez dostawcę w imieniu klienta, takich jak dostęp do kluczy szyfrujących klienta. W środowisku w chmurze istnieje jednak ważne, nowe źródło dzienników uprzywilejowanego użytkownika: możliwe jest śledzenie działań zespołu, korzystając z portali dostawcy, interfejsów API i interfejsów wiersza polecenia.

W środowisku w chmurze nie istnieje możliwość kontaktu z fizycznym sprzętem. Wiele zespołów reagujących na incydenty wyposażonych jest w podręczne torby zawierające specjalistyczny sprzęt, taki jak laptopy kryminalistyczne, powielacze dysków twardych. Tego typu sprzęt może być potrzebny w przypadku incydentów związanych z infrastrukturą niebędącą chmurą, na przykład w przypadku zawirusowanego oprogramowania

na laptopach pracowników. Do reagowania na incydenty w środowisku w chmurze konieczne jest posiadania wirtualnego odpowiednika takich narzędzi. Oznacza to także, że częściowe reakcje na incydenty w chmurze mogą zostać przeprowadzone z dowolnego miejsca, aczkolwiek fizyczna kolokacja z innymi osobami zaangażowanymi w ten incydent może nadal przynosić znaczące korzyści.

Co monitorować

Każdy system o rozsądnej wielkości oferuje tak wiele różnych dzienników i mierników, że łatwo jest zostać pogrzebanym w danych, które niekoniecznie mogą być przydatne do celów bezpieczeństwa. Wybór tego, co ma być monitorowane, jest bardzo ważny! Niestety muszą to być elementy specyficzne dla użytkowanego środowiska i aplikacji. Konieczne jest więc sprecyzowanie modelu zagrożeń: określenie posiadanych zasobów i tego, kto najprawdopodobniej może je zaatakować, oraz określenie, jakie dzienniki wychodzą z systemów w pipeline zarządzania zasobami, co zostało omówione w rozdziale 3.

Na przykład w przypadku posiadania terabajtów danych, obserwowanie metryk dotyczących natężenia ruchu sieciowego i długości połączeń może być bardzo przydatne w celu nakrycia kogoś na kradzieży. Jednakże tego typu dane o ruchu w sieci nie będą przydatne, jeśli rozpowszechniane jest oprogramowanie z zaimplementowanym backdoorem. W takim przypadku ilość danych, miejsce docelowe i długość sesji nie ulegną zmianie, ale treść zostanie uszkodzona.

Na przykład w momencie, gdy zostało zakupione określone narzędzie, takie jak oprogramowanie antywirusowe (AV), oraz upewniono się, że jest uruchomione na wszystkich maszynach wirtualnych w chmurze, głupotą jest ignorowanie powiadomień z takiego narzędzia. Powiadomienie takie może oznaczać, że narzędzie mogło dokonać pomyślnej ochrony przed całym atakiem. Ewentualnie mogło dojść do blokady jedynie części ataku lub wykrycia czegoś podejrzanego, co jednak nie zostało zablokowane. Konieczne jest więc sprawdzanie, w jaki sposób złośliwe oprogramowanie dostało się do systemu i czy atak został całkowicie zablokowany, czy też nie.

Poniżej przedstawiono kilka ogólnych punktów wyjścia do tego, co warto monitorować, po uprzednim określeniu modelu zagrożenia oraz komponentów, jakie wchodzą w skład używanego środowiska. Zostały one wymienione w przybliżeniu w porządku priorytetowym, choć oczywiście zależy to w dużej mierze od używanego środowiska. Bardziej konkretne przykłady zostały omówione na końcu tego rozdziału, w części poświęconej przykładowej aplikacji.

Dzienniki, zdarzenia, powiadomienia i mierniki

Dziennik lub *zdarzenie* to zapis konkretnego wydarzenia. Na przykład w środowisku może być generowany rekord dziennika za każdym razem, gdy ktoś uwierzytelnia się, wysyła żądanie sieciowe, zużycie procesora wzrasta przez pięć minut lub dowolną liczbę innych rzeczy, które mogą się zdarzyć w złożonym środowisku.

Powiadomienie to rodzaj zdarzenia, o którym warto jest kogoś powiadomić. Fakt pobrania przez oprogramowanie antywirusowe aktualizacji definicji jest zdarzeniem. Zdarzenie polegające na faktycznym znalezieniu złośliwego oprogramowania powinno być powiadomieniem!

Miernik to zestaw liczb, które zawierają informacje o czymś. Metryki są zwykle oparte na czasie, tak więc możliwe jest gromadzenie mierników co minutę, na przykład określających liczbę żądań uwierzytelnienia, ilość dostępnego wolnego miejsca na dysku lub liczbę wykonanych żądań internetowych.

Podstawową zaletą dzienników jest to, że dostarczają one bardzo dużo informacji o tym, co się wydarzyło, aczkolwiek koszt przechowywania i przeszukiwania dzienników może szybko wzrosnąć wraz ze wzrostem aktywności. Jeśli liczba żądań internetowych wzrośnie dwa razy, to także liczba rekordów w dzienniku wzrośnie dwukrotnie! Z drugiej strony, wartości mierników będą wzrastały w każdym kolejnym okresie wraz ze wzrostem aktywności, ale koszt przechowywania i przetwarzania takich danych nie ulegnie zmianie, ponieważ do przechowywania liczb „100" i „200" zwykle potrzeba tyle samo miejsca. Zarówno dzienniki, jak i mierniki mogą być przydatne do wykrywania incydentów związanych z bezpieczeństwem i generowania powiadomień. W przypadku gdy jest zbyt wiele pozycji dziennika do przeszukania, mierniki mogą być lepszym wyborem do tworzenia powiadomień.

W przypadku każdego rodzaju zdarzeń należy upewnić się, że wpisy dziennika zawierają wystarczającą ilość danych, tak aby były przydatne. Zazwyczaj oznacza to co najmniej, *kiedy*, *co* i *kto*: kiedy zdarzenie się wydarzyło, co się wydarzyło i kto je wywołał. W niektórych przypadkach „kto" może być systemem lub innym automatycznym narzędziem, na przykład w momencie zgłoszenia przez system dużego użycia procesora.

Poza jednym wyjątkiem nigdy nie należy umieszczać haseł, kluczy API, wrażliwych danych osobowych, chronionych informacji zdrowotnych lub wszelkich innych wrażliwych danych w dziennikach. W większości przypadków nie każda osoba, która ma dostęp do dzienników, jest upoważniona do przeglądania tych informacji. Ponadto, posiadanie kopii poufnych informacji w większej liczbie miejsc, niż jest to konieczne, zwiększa ryzyko przypadkowego ujawnienia tych danych.

W rzeczywistości, ze względu na prywatność, należy unikać bezpośredniego rejestrowania danych umożliwiających identyfikację osób, o ile jest to tylko możliwe. W przypadku chęci dowiedzenia się, kto został wymieniony w dziennikach, należy użyć unikatowych identyfikatorów, takich jak GUID, a nie danych osobowych. Tabela, która pozwala skorelować te identyfikatory GUID z rzeczywistymi obiektami, powinna być przechowywana w innym miejscu.

PWNING_WEEK 2021

Dołącz do uczestników PWNing Week 2021!

Grupa PWN zaprasza do udziału w **PWNing Week 2021** – jednym z ważniejszych w Polsce wydarzeń z obszaru cyberbezpieczeństwa. Tegoroczna edycja odbędzie się online i jest rozszerzoną formułą odbywającej się w ubiegłych latach konferencji **Security PWNing**.

Dowiedz się więcej

Tegoroczną edycję kierujemy szczególnie do kadry zarządzającej, osób odpowiedzialnych za wybór i zakup rozwiązań z zakresu bezpieczeństwa i monitoringu sieci oraz poszukujących nowych rozwiązań chmurowych.

PWNing WEEK 2021 to:

- Security Conference (17-19 listopada)
- strefa EXPO (17-19 listopada)
- warsztaty, szkolenia i inne wydarzenia towarzyszące (15-16 listopada, 22-26 listopada)

Tematyka PWNing Security Conference:

- Bezpieczeństwo danych w dobie pandemii i masowej pracy zdalnej
- Rozwiązania chmurowe
- Narzędzia wspomagające bezpieczeństwo danych

Zarejestruj się

Konferencję poprowadzi dla Was
dr Maciej Kawecki

Wyjątkiem od reguły dotyczącej poufnych danych w dziennikach jest nagrywanie sesji, które mogą rejestrować hasła lub inne poufne informacje, w celu monitorowania użytkowników uprzywilejowanych. W takim przypadku dostęp do rekordów sesji musi być bardzo ściśle kontrolowany, ale korzyści wynikające z możliwości kontrolowania uprzywilejowanych użytkowników często przewyższają ryzyko posiadania sekretów w tych rekordach.

Dostęp użytkownika uprzywilejowanego

Prawie wszyscy powinni rejestrować, a przynajmniej sprawdzać na miejscu, logowania użytkowników uprzywilejowanych na wszystkich poziomach środowiska. Przeglądanie takich dzienników może być świetnym sposobem na postawienie pytań prowadzących do wykrycia złośliwej aktywności, takich jak: „Dlaczego ta osoba w ogóle się loguje?" lub „Czy ta osoba nie opuściła firmy?" lub „Czy ktoś rozpoznaje to konto?".

Monitorowanie dostępu użytkowników uprzywilejowanych nie jest równoznaczne z brakiem zaufania do administratorów. W idealnym świecie nie ma konieczności ufania w 100% każdej osobie. W przeciwnym razie do wykonania każdego zadania konieczne byłyby co najmniej dwie osoby, które wiedziałyby o wykonywaniu tego zadania i musiałyby być w zmowie, w celu wykonania zadania bez wykrycia[1]. Taki poziom staranności z pewnością nie jest konieczny dla wszystkich zadań w większości organizacji, aczkolwiek może zostać uwzględniony w przypadku działań o wysokiej wartości, takich jak przekazy pieniężne lub dostęp do tajnych magazynów danych. To, na czym należy się głównie skoncentrować, to wykrywanie nieautoryzowanej osoby udającej administratora. Biorąc pod uwagę, że jedną z najczęstszych przyczyn incydentów związanych z bezpieczeństwem jest zagubienie lub kradzież danych uwierzytelniających, obserwowanie tego, co robią administratorzy, to świetny sposób na złapanie kogoś *udającego* administratora.

Dostawcy usług w chmurze mogą oferować szczegółowe zapisy w dziennikach dotyczące logowania na konta administratorów za pomocą interfejsów administracyjnych w chmurze (portal internetowy, interfejsy API lub interfejsy wiersza polecenia), a także wykonanych czynności. Na przykład mogą zostać wyświetlone rekordy, takie jak „utworzył instancję", „utworzył bazę danych" lub „utworzył użytkownika administracyjnego". Dzienniki te mogą być gromadzone przez usługi w chmurze, takie jak AWS CloudTrail, Azure Activity Log, Google Stackdriver Logging i IBM Cloud Activity Tracker. W niektórych przypadkach jednak może być konieczne jawne włączenie funkcji rejestrowania, określenie miejsca i czasu przechowywania dzienników oraz zapłacenie za przechowywanie.

Oprócz dostępu do dzienników użytkowników uprzywilejowanych gromadzonych przez dostawcę chmury, administratorzy często mają również uprzywilejowany dostęp do systemów tworzonych w środowisku w chmurze. Na przykład możliwe jest posiadanie kont administracyjnych do maszyn wirtualnych, urządzeń zapory lub baz danych. Dostęp do nich może być zgłaszany za pomocą protokołu, takiego jak syslog. Administratorzy

[1] Jest to czasem nazywane „zasadą czterech oczu" lub „zasadą dwóch osób".

mogą wykorzystywać także inne systemy, takie jak przechowalnia haseł do sprawdzania wspólnych identyfikatorów. Ogólnie rzecz biorąc, wszystkie systemy używane przez administratorów do wykonywania działań uprzywilejowanych powinny rejestrować te działania w celu późniejszej kontroli.

Dzienniki aktywności administracyjnej powinny być podzielone na dwa typy, które zostały oznaczone jako dzienniki pełne i pozbawione poufnych informacji.

Dzienniki pełne mogą zawierać sekretne informacje, takie jak hasła i klucze API, które mogłyby umożliwić osobie atakującej bezpośredni dostęp do systemu. Możliwe jest nieposiadanie żadnych pełnych dzienników w używanym środowisku. Zasadniczo dostęp do tego typu dzienników powinien być możliwy tylko podczas podejrzewanego incydentu lub dostęp powinien mieć niewielki, monitorowany zespół, który regularnie sprawdza sesje administracyjne. Uzyskanie dostępu do pełnych dzienników powinno wywoływać pewną formę powiadomienia, tak aby co najmniej dwie osoby wiedziały, że dzienniki takie zostały udostępnione. Poniżej wymieniono kilka przykładów pełnych dzienników:

- Bezpieczne dzienniki sesji Shell lub inne dzienniki zawierające polecenia i opcje.
- Dziennik dokładnych poleceń wykonanych przez administratorów na maszynach wirtualnych za pośrednictwem funkcjonalności dostawcy usług w chmurze, takiej jak Amazon EC2 Run Command, chyba że posiadany jest jakiś sposób na pomijanie sekretów podczas rejestracji poleceń.
- Dziennik dokładnych poleceń wykonanych przez administratorów na kontenerach, taki jak te zaczynające się od *kubectl exec*, chyba że posiadany jest jakiś sposób na pomijanie sekretów podczas rejestracji poleceń.

Dzienniki pozbawione poufnych informacji zostały specjalnie zaprojektowane tak, aby nie zawierać sekretów. Zdecydowana większość dzienników powinna należeć do tej kategorii. Poniżej wymieniono kilka przykładów dzienników pozbawionych poufnych informacji:

- Dziennik działań wykonanych przez administratorów za pośrednictwem interfejsu API w chmurze lub konsoli dostawcy chmury.
- Dziennik działań wykonanych przez administratorów na konsoli Kubernetes, takich jak wdrażanie nowych aplikacji lub autoryzowanie dodatkowych użytkowników.
- Dziennik pomyślnych oraz nieudanych prób uwierzytelnienia i autoryzacji dowolnego z elementów systemu. Na przykład w przypadku pomyślnego zalogowania się do konsoli w chmurze przez administratora, który nie ma autoryzacji do utworzenia tam zasobu, oba zdarzenia powinny zostać zarejestrowane.

Dzienniki narzędzi defensywnych

W przypadku używania narzędzi obronnych, takich jak oprogramowanie antywirusowe, zapory sieciowe, zapory aplikacji internetowych, systemy wykrywania włamań lub narzędzia do monitorowania sieci, konieczne jest przeglądanie dzienników pochodzących

z tych narzędzi. Nie można być pewnym, że narzędzia te są w 100% skuteczne w zapobieganiu wszystkim atakom. W niektórych przypadkach narzędzia mogą zablokować początkowy atak, ale przepuszczać kolejny lub jedynie rejestrować wydarzenie bez zablokowania ataku. Konieczne jest zbieranie oraz analizowanie dzienników z tych usług w przeciwnym razie niwelowana jest zaleta wczesnego ostrzegania.

Problematyczne może być to, że niektóre z tych narzędzi mogą charakteryzować się wysokim odsetkiem alarmów fałszywie pozytywnych. Nie należy jednak lekceważyć ryzyka tego typu alarmów! Bardzo łatwo jest wyszkolić siebie i swoich pracowników w zakresie ignorowania powiadomień, które mogą być naprawdę ważne. Konieczne jest wykorzystanie pętli sprzężenia zwrotnego, tak aby osoby obserwujące fałszywe alarmy mogły próbować albo całkowicie odfiltrować określone dzienniki z przetwarzania, ewentualnie dostroić system w celu zmniejszenia liczby generowanych fałszywych alarmów. Zadanie takie oczywiście jest pewną sztuką, ponieważ istnieje ryzyko odfiltrowania oraz eliminowania powiadomień prawdziwie pozytywnych, aczkolwiek w większości przypadków powinno się zaakceptować bardzo małe ryzyko w celu uniknięcia ignorowania powiadomień. Podobnie jak powinno się mieć wiele warstw ochrony, powinno się także mieć wiele warstw wykrywania, tak aby nie być zależnym tylko od jednego narzędzia do wykrywania złośliwej aktywności.

Zalecenia dotyczące rejestrowania w przypadku większości narzędzi defensywnych w środowisku w chmurze są bardzo podobne do tych w środowiskach lokalnych.

Anty-DDoS

Systemy używane do obrony przed atakami typu DDoS powinny być skonfigurowane w taki sposób, aby ostrzegały przed atakami, ponieważ mogą się one z czasem nasilać lub wskazywać na prawdopodobieństwo naruszenia. Ponadto atak DDoS może odgrywać rolę zasłony dymnej mającej na celu ukrycie innych działań, związanych z naruszeniem, chociaż nie ma zgody co do tego, jak często występuje coś takiego[2].

Zapory sieciowe aplikacji internetowych

Zarówno rozproszone, jak i scentralizowane rozwiązania WAF mogą ostrzegać o atakach, które zostały zablokowane lub o podejrzanych żądaniach. Powiadomienia takie mogą być przydatne do zrozumienia, kiedy została podjęta próba ataku na aplikacje internetowe.

Do certyfikacji PCI DSS często wykorzystuje się WAF zamiast ręcznych przeglądów kodów. W związku z tym należy także wykazać, że dzienniki z systemów WAF są przechowywane i analizowane.

[2] W raporcie Worldwide DDoS Attacks & Cyber Insights Research Report z 2017 r. (*https://www.discover.neustar/201705-Security-Solutions-DDoS-SOC-Report-LP.html*) stwierdzono, że „ataki DDoS były często stosowane w połączeniu z innymi działaniami związanymi z cyberprzestępczością", podczas gdy w raporcie Verizon Data Breach Investigations Report (*http://bit.ly/2bOqPlj*) stwierdzono: „nigdy nie mieliśmy roku z więcej niż jednocyfrowymi naruszeniami według wzoru Denial of Service." Warto jednak zauważyć, że pierwszy raport został wydany przez dostawcę anty-DDoS.

Zapory sieciowe i systemy wykrywania włamań

Zapory sieciowe skierowane do internetu oraz systemy IDS (ang. *Intrusion Detection Systems*) muszą być odpowiednio dostrojone, ze względu na to, że systemy są stale narażone na ataki niskiej jakości, takie jak skanowanie portów i zgadywanie haseł. Dane historyczne dostarczone przez takie systemy mogą jednak być przydatne w przypadku podejrzewanego incydentu.

Z drugiej strony, zapora sieciowa lub system IDS wdrożone w obwodzie powinny zostać dostrojone tak, aby były wrażliwe, ponieważ powiadomienia sygnalizowane w tym miejscu najprawdopodobniej są związane z błędną konfiguracją lub faktycznym atakiem. Oprócz innych narzędzi defensywnych, które mogą zostać umieszczone na białej liście, tak aby nie powodowały powiadomień, nic innego nie powinno tak naprawdę skanować sieci wewnętrznej ani powodować nieudanych połączeń.

Do tej samej, ogólnej kategorii można zaliczyć także systemy *analizy ruchu sieciowego*, które zazwyczaj są wykorzystywane do agregacji danych dotyczących przepływu z routerów i przełączników w celu uzyskania całościowego obrazu przemieszczania się danych do, z i przez środowisko. Narzędzie te również mogą być konfigurowane w celu wysyłania powiadomień wskazujących na nieprawidłowości.

Programy antywirusowe

Należy upewnić się, że otrzymywane będą powiadomienia, jeśli w jakichkolwiek systemach w systemie zarządzania zasobami nie zostanie uruchomione oprogramowanie AV oraz jeśli zostanie wykryte złośliwe oprogramowanie.

Należy pamiętać, że jedną z pierwszych czynności wykonywanych przez atakujących, którzy wykorzystują luki w celu dostania się do systemu, jest zazwyczaj instalacja złośliwego oprogramowania w systemie.

W przypadku ataku przez inteligentnych atakujących najprawdopodobniej zostanie wykorzystane niestandardowe złośliwe oprogramowanie, tak aby jego użycie nie wywołało powiadomienia używanego oprogramowania antywirusowego. Atakujący tacy mogą korzystać z usług lub być w posiadaniu laboratoriów do sprawdzenia, czy jakiekolwiek dostępne oprogramowanie AV jest w stanie wykryć złośliwe oprogramowanie, którego zamierzają potem użyć. Na szczęście nie wszyscy atakujący są tak sprytni, a oprogramowanie antywirusowe jest nadal bardzo pomocne w wykrywaniu tych mniej sprytnych. Nie należy odrzucać narzędzi tylko dlatego, że nie są one w 100% skuteczne!

Podczas niesławnego naruszenia danych klientów sieci Target w 2013 roku jednym z błędów był brak reakcji na powiadomienia z oprogramowania antywirusowego.

Wykrywanie stacji końcowych i reagowanie na incydenty

Tam, gdzie tradycyjne oprogramowanie antywirusowe jest skoncentrowane głównie na blokowaniu złośliwej aktywności, oprogramowanie do *wykrywania punktów końcowych i reagowania* (EDR, ang. *Endpoint Detection and Response*) jest bardziej skoncentrowane na umożliwieniu zespołom badania i reagowania na zagrożenia, które przeszły przez pierwszą linię obrony. Jeśli porównać AV z materiałami zmniejszającymi palność w strukturze fizycznej, to oprogramowanie EDR jest podobne do czujników dymu i systemów zraszaczy.

Działanie EDR polega zwykle na rejestrowaniu dużej ilości informacji o uruchomionych systemach, takich jak wartości skrótu każdego pliku wykonywalnego lub biblioteki uruchomionej w systemie, lub historia prób nawiązania lub nawiązanych połączeń sieciowych. Mimo że możliwe jest uzyskanie niektórych z tych informacji za pomocą dzienników systemu operacyjnego lub sieci, wykorzystując oprogramowanie EDR, łatwo jest je zgromadzić w jednym miejscu. Następnie informacje takie mogą być łatwo powiązane ze źródłami informacji o zagrożeniach, takimi jak nowo odkryte serwery zarządzania i kontroli lub nowo zgłoszone sygnatury złośliwego oprogramowania, w celu wykrycia zarówno bieżącej, jak i historycznej aktywności. Niektóre oprogramowanie EDR można również wykorzystać do kwarantanny i badania systemów w przypadku wykrycia ataku.

Podczas gdy funkcjonalności te są często wykorzystywane interaktywnie przez zespół reagujący, rozwiązania EDR mogą również wysyłać powiadomienia w przypadku wykrycia zagrożeń w środowisku, tak więc w pewnym stopniu pokrywają się z oprogramowaniem antywirusowym.

Monitorowanie integralności plików

Niektóre pliki nie powinny się regularnie zmieniać, a jeśli zostaną zmienione, może to świadczyć o ataku. Na przykład, jeśli modyfikacji ulegnie konfiguracja systemu rejestrowania, może to być podejrzane. W rzeczywistości, w systemie Linux większość zmian w drzewie katalogów */etc* należy przeglądać z pewną podejrzliwością.

Oprogramowanie do *monitorowania integralności plików* (FIM, ang. *File Integrity Monitoring*) może powiadamiać o zmianie określonych plików, a niektóre produkty umożliwiają także powiadamianie o zmianie niektórych wpisów rejestru systemu Windows. W ofercie niektórych dostawców chmury oprogramowanie FIM występuje jako część platformy zarządzania chmurą IaaS. Istnieją również bezpłatne i płatne wersje produktów FIM, które mogą zostać wdrożone we własnych systemach.

Monitorowanie integralności plików jest wyraźnie wymagane do certyfikacji PCI DSS, a według niektórych audytorów wymagane jest, aby obejmowało nie tylko pliki płaskie, ale także zmiany w rejestrze systemu Windows.

Dzienniki i mierniki usług w chmurze

Oprócz rejestrowania działań administracyjnych większość dostawców usług w chmurze ma w ofercie także przydatne dzienniki i mierniki dotyczące swoich usług w chmurze. Należy przejrzeć dzienniki oraz metryki dotyczące wykorzystywanych usług w chmurze i zdecydować, które z nich mogą być wykorzystane do sygnalizacji ataku i/lub być przydatne w ustaleniu negatywnych skutków ataku. Poniżej przedstawiono kilka przykładów:

Mierniki wykorzystania procesora
: Skoki wykorzystania procesora, niewyjaśnione przez zwiększone użycie, mogą wskazywać na aktywne szyfrowanie ransomware lub „kopanie" kryptowalut.

Dzienniki i mierniki sieciowe
: Na przykład, jeśli wykorzystywane są wirtualne podsieci chmury prywatnej, wielu dostawców chmury może dostarczać mierniki dotyczące danych wchodzących i wychodzących z tych podsieci, a także dzienniki przepływu ruchu zaakceptowanego i zabronionego. Odmowa ruchu, gdy źródłem jest własny komponent, może wskazywać na błędną konfigurację lub atak i powinna zostać zbadana. Skoki ruchu sieciowego mogą z kolei wskazywać na rozpoczęcie ataku typu DDoS lub na postępującą kradzież danych przez osobę atakującą.

Dane wejściowe/wyjściowe pamięci masowej
: Skokowy wzrost wejścia/wyjścia, niewyjaśniony zwiększonym wykorzystaniem, może wskazywać na aktywne oprogramowanie ransomware, atak typu DDos lub na postępującą kradzież danych przez osobę atakującą.

Dane dotyczące żądań do komponentów platformy, takich jak bazy danych lub kolejki komunikatów
: W przypadku zaobserwowania dziwnych zachowań w bazie danych może to oznaczać fakt kradzieży znacznych ilości danych. Jeśli zaś dziwne zachowania obserwowane są w kolejkach wiadomości, może to sugerować, że w pewnej części systemu obecna jest osoba atakująca, próbująca wysyłać wiadomości do innych komponentów.

Logowania użytkowników końcowych i aktywność w ofertach SaaS
: W przypadku gdy użytkownik zacznie pobierać ogromne ilości danych z usługi pamięci masowej w chmurze, może to oznaczać, że konto zostało przejęte. Możliwe jest również monitorowanie szczegółowych zdarzeń związanych z aktywnością użytkowników, które mogą być generowane w przypadku wykorzystywania brokera zabezpieczeń dostępu do chmury (CASB, ang. *Cloud Access Security Broker*) do pośredniczenia w dostępie do usługi w chmurze.

Dzienniki i mierniki usług platformy
: Każda usługa platformy może oferować dzienniki i mierniki, które oprócz monitorowania operacyjnego są przydatne do wykrywania i reagowania. Na przykład, jeśli wykorzystywana jest platforma taka jak Kubernetes, możliwe jest włączenie

inspekcji. W dokumentacji Kubernetes (*https://kubernetes.io/docs/tasks/debug-application-cluster/audit/*) zostało wyjaśnione, jak włączyć rejestrowanie kontroli i jak przesyłać takie dzienniki do punktu zbiorczego. W przypadku pamięci obiektów, baz danych i innych usług w chmurze również oferowane są dzienniki i mierniki specyficzne dla danej usługi.

Dzienniki i mierniki systemu operacyjnego

W przypadku użytkowania maszyn wirtualnych lub maszyn typu bare-metal w chmurze, na ogół odpowiedzialność za bezpieczeństwo systemu operacyjnego obejmuje gromadzenie i analizowanie dzienników. Jest to postępowanie podobne do tego stosowanego w przypadku infrastruktury lokalnej:

- Lista CIS Benchmarks (*https://www.cisecurity.org/cis-benchmarks/*) to rozsądny podstawowy zestaw zdarzeń do rejestrowania wielu różnych systemów operacyjnych, produktów i usług, z których może się składać środowisko.
- W przypadku korzystania z systemu Windows zostały udostępnione przez Microsoft informacje o identyfikatorach zdarzeń, które należy monitorować. Na przykład dla dość powszechnego rodzaju ataku typu pass-the-hash udostępniona jest dokumentacja (*https://www.microsoft.com/en-us/download/details.aspx?id=36036*) zawierająca informacje o określonych identyfikatorach zdarzeń, które należy monitorować w celu wykrycia takiego ataku.
- Dla użytkowników Linuxa zostały udostępnione przez wielu dostawców tego systemu instrukcje, jak włączyć rejestrowanie kontroli, aby spełnić różne wymagania branżowe i prawne. Nawet jeśli nie jest wymagane spełnienie tych wymagań, instrukcje mogą być przydatnym punktem wyjścia do rejestrowania i analizowania w używanym środowisku.
- Mierniki, takie jak zużycie pamięci, użycie procesora i operacje wejścia/wyjścia, mogą być bardzo przydatne dla zespołów do spraw bezpieczeństwa oraz zespołów operacyjnych.

Dzienniki oprogramowania pośredniczącego

W przypadku używania własnej bazy danych, menedżera kolejek, serwera aplikacji lub innego oprogramowania pośredniczącego, konieczne może być włączenie rejestrowania i gromadzenia danych. Oprócz wszelkich działań użytkowników uprzywilejowanych (patrz „Dostęp użytkownika uprzywilejowanego” na stronie 147), możliwe jest skonfigurowanie: powiadomień dotyczących wszelkiego dostępu do poufnych baz danych, który pochodzi z dowolnego miejsca oprócz legalnego identyfikatora aplikacji lub systemu, powiadomień dostępu do określonych tabel lub innych powiadomień przydatnych do śledzenia dostępu do wrażliwych danych.

Serwer sekretów

Jeśli wykorzystywany jest serwer sekretów, tak jak zostało to omówione w rozdziale 4, powinno się rejestrować cały dostęp do sekretów. Oto kilka przykładów nietypowych działań, o których należy alarmować i które należy analizować:

- Niepowodzenie uwierzytelnienia lub autoryzacji na serwerze sekretów, co może wskazywać na atak.
- Niezwykła aktywność w wyszukiwaniu sekretów.
- Wykorzystanie poświadczeń administracyjnych.

Twoja aplikacja

W przypadku wykorzystywania niestandardowej aplikacji lub aplikacji innej firmy mogą być tworzone ich własne dzienniki i dane, które mogą być przydatne zarówno dla zespołów operacyjnych, jak i zespołów do spraw bezpieczeństwa. Na przykład podczas używania aplikacji bankowej mogą być rejestrowane wszystkie przelewy, a w przypadku przelewów powyżej określonej wartości mogą być generowane powiadomienia.

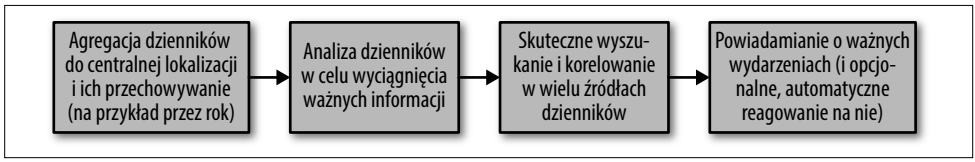
Techniki oszustwa

Oprócz różnych technologii wykrywania dostępne są też takie, które mają na celu utrudnić życie atakującym bez przeszkadzania zwykłym użytkownikom i administratorom. Najczęstszym przykładem takiego narzędzia jest *honeypot*, który jest systemem udającym funkcjonalną część infrastruktury, ale mającym na celu jedynie odwracanie uwagi, spowalnianie atakujących oraz ostrzeganie, gdy włamią się do systemu.

Technologie oszukiwania mogą być użytecznym sposobem na wykorzystanie „przewagi sądu domowego" w obronie środowiska, ponieważ możliwe jest zastawianie pułapek na atakujących, znanych tylko właścicielowi środowiska. Jest to jednak technika zaawansowana. Przed zainwestowaniem czasu i wysiłku w techniki oszukiwania należy upewnić się, że dysponuje się skutecznie działającymi planami rejestrowania, monitorowania, ostrzegania, reagowania i odzyskiwania.

Jak monitorować?

Po omówieniu rodzajów zdarzeń oraz mierników, które warto obserwować w używanym środowisku, kolejnym etapem jest omówienie, jak skutecznie zbierać je i wykorzystywać do wykrywania włamań i reagowania na nie. Na rysunku 7.1 pokazano różne etapy tego procesu. Kroki te mogą być wykonane przez pojedynczy produkt lub usługę, taką jak SIEM, lub przez wiele produktów i usług działających razem.



Rysunek 7.1. Łańcuch rejestrowania i ostrzegania

Należy upewnić się, że we wszystkich systemach dokonano synchronizacji czasu, zazwyczaj za pomocą protokołu Network Time Protocol (NTP). Ponadto należy upewnić się, że wszystkie znaczniki czasu zawierają informacje o strefie czasowej lub używana jest ta sama strefa czasowa (np. GMT) dla wszystkich dzienników. Jest to zazwyczaj bardzo łatwe do skonfigurowania, a koszmarem może być korelowanie zdarzeń między różnymi źródłami dziennika w momencie, gdy zegary systemowe lub strefy czasowe są wyłączone.

Agregacja i zatrzymywanie

Wszystkie opisane wcześniej dzienniki muszą być gdzieś magazynowane i przechowywane przez minimalną ilość czasu. Mimo że zezwalanie na gromadzenie dzienników w różnych systemach jest o wiele lepsze niż brak dzienników, jest to postępowanie dalekie od ideału. Poszczególne dyski systemowe mogą się zapełniać, powodując utratę logów oraz problemy operacyjne, a osoba atakująca, która dostanie się do systemu, może także usunąć dzienniki w celu zamaskowania śladów włamania. Ponadto korzystanie z dziesiątek różnych systemów w celu przeszukiwania dzienników i zbierania obrazu tego, co się dzieje, może być bardzo niewygodne i czasochłonne.

W przeszłości ważne dzienniki często drukowano na papierze i wysyłano do fizycznie bezpiecznego miejsca. Mimo że jest to dość bezpieczny sposób ich zabezpieczania oraz zapobiegania przed skasowaniem przez komputer, papier ma pewne poważne wady: nie ma możliwości automatycznego przeszukiwania, jest ciężki, drogi i stanowi zagrożenie pożarowe.

W chmurze możliwe jest znacznie łatwiejsze uzyskanie takich samych korzyści, lokalizując usługę agregacji dzienników na osobnym koncie w chmurze z innymi administracyjnymi danymi uwierzytelniającymi tak, aby dzienniki nie mogły zostać usunięte przez osobę mającą dostęp do systemów podstawowych. Postępowanie takie jest również dobrym pomysłem na tworzenie kopii zapasowych, co zostało omówione w dalszej części. Większość dostawców usług w chmurze ma w ofercie usługi, które mogą zostać wykorzystane do agregacji, przechowywania oraz przeszukiwania dzienników, tak więc nie istnieje potrzeba konfigurowania agregacji dzienników od zera.

Większość dzienników należy przechowywać przez co najmniej rok, chociaż dzienniki przechowywane przez dłuższe okresy mogą czasem być pomocne w badaniu incydentów bezpieczeństwa. W przypadku podlegania jakimkolwiek normom branżowym lub regulacyjnym należy zapoznać się ze szczegółowymi wymogami dotyczącymi przechowywania tych dzienników, aczkolwiek zazwyczaj wystarczającym okresem jest jeden rok.

Po umieszczeniu wszystkich dzienników i powiadomień w centralnej, bezpiecznej lokalizacji z odpowiednim okresem przechowywania, konieczne jest rozwiązanie problemu z przeglądaniem tych dzienników w celu powiadamiania o podejrzanym zachowaniu oraz upewnienia się, że powiadomienia trafiają do odpowiednich osób, są potwierdzone i zbadane.

Parsowanie

W momencie, gdy wszystkie dzienniki zostaną już zebrane w bezpiecznym miejscu, można sobie pogratulować! Zdeterminowana osoba może w końcu przejrzeć wszystkie dzienniki i uzyskać odpowiedzi na ważne pytania, choć może to być czasochłonne. Jednakże, jedną z głównych motywacji do wynalezienia komputerów było przetwarzanie danych znacznie szybciej, niż są to stanie zrobić ludzie.

Parsery dzienników są wykorzystywane do wyciągania określonego typu informacji (pola) z różnych typów zdarzeń. Poniżej przedstawiono kilka przykładów działania parserów:

- W przypadku zdarzenia systemu operacyjnego analizator składniowy jest wykorzystywany do rozpoznania znacznika czasu, nazwy systemu generującego zdarzenie oraz tekstu zdarzenia. Dalsza analiza może nastąpić w przypadku niektórych typów zdarzeń. Na przykład w przypadku nieudanego zdarzenia logowania analizator może również rozpoznać adres IP, z którego próbowano się zalogować.
- W przypadku dzienników zapory analizator składniowy jest wykorzystywany do rozpoznania znacznika czasu, źródłowego adresu IP, docelowego adresu IP oraz rezultatu połączenia: zaakceptowane/odrzucone.
- W przypadku dzienników programów antywirusowych analizator składniowy jest wykorzystywany do rozpoznania znacznika czasu, nazwy hosta oraz szczegółów zdarzenia, takich jak nieudana aktualizacja lub wykrycie złośliwego oprogramowania.

Niestety dzienniki mogą występować w tysiącach różnych formatów. Istnieje jednak kilka popularnych formatów dzienników zdarzeń, które ułatwiają analizę składniową. Wiele narzędzi może przetwarzać dzienniki w tych formatach na określone pola, choć nie zawsze oznacza to, że pola te będą przydatne. Poniżej przedstawiono kilka przykładów:

- Syslog to standardowy format długich wiadomości, chociaż określenie „format" jest nieco przesadzone[3]. W rzeczywistości istnieje kilka popularnych formatów syslog: RFC 3164 (*https://tools.ietf.org/html/rfc3164*) opisujący zbiór wolno występujących rzeczy, podczas gdy RFC 5424 (*https://tools.ietf.org/html/rfc5424*) jest bardziej nakazowy. Zazwyczaj rekord syslog zawiera znacznik czasu, nazwę systemu generującego wiadomość, rodzaj procesu wysyłającego wiadomość, poziom istotności oraz wiadomość w dowolnej postaci. Często analizator składniowy musi zdobyć informację o tym, co wygenerowało taką wiadomość i przeprowadzić dalszą jego analizę.
- Common Log Format (CLF) i Extended Log Format (ELF) są używane głównie przez serwery sieciowe do rejestrowania żądań.
- Common Event Format (*https://community.softwaregrp.com/t5/ArcSight-Connectors/ArcSight-Common-Event-Format-CEF-Implementation-Standard/ta-p/1645557*) (CEF) jest rozszerzeniem formatu syslog, używanym głównie przez MicroFocus ArcSight, który zapewnia dodatkowe pola strukturalne.
- Standard Cloud Audit Data Federation (*https://bit.ly/2RT9JHb*) (CADF) ma na celu umożliwienie przełączania się między dostawcami usług w chmurze bez zmiany systemów agregacji dzienników i analizy składni.

Wyszukiwanie i korelacja

Po zebraniu i poddaniu dzienników analizie składniowej możliwe jest dalsze wyszukiwanie na podstawie pól analizy składniowej i korelowanie zdarzeń między różnymi systemami. Na przykład możliwe jest wyszukanie: wszystkich nieudanych prób logowania w określonym czasie, wszystkich przypadków pomyślnego logowania bez połączenia VPN dla tego samego użytkownika lub zdarzeń polegających na wykryciu złośliwego oprogramowania po zalogowaniu.

Możliwość szybkiego wyszukiwania w wielu różnych źródłach i typach dzienników może być nieoceniona podczas reagowania na incydent. System powinien zostać przetestowany, jak sprawnie jest w stanie przeprowadzać wiele zwariowanych wyszukiwań, przed nastąpieniem incydentu związanego z bezpieczeństwem!

Wiele systemów oferuje możliwość przechowywania w trybie *hot storage* i *cold storage*. Przechowywanie w trybie „hot" może być sprawdzane natychmiast, natomiast w przypadku przechowywania w trybie „cold" wymagane jest odzyskanie i ponowne załadowanie, zanim możliwe będzie ich przeszukanie.

[3] Termin „syslog" może być mylący, ponieważ jest często używany w odniesieniu do programu do przyjmowania wiadomości syslog, protokołu sieciowego (zwykle działającego na udp/514 lub tcp/514) oraz formatu wierszy w pliku dziennika.

Alarmowanie i automatyczna reakcja

W przypadku wykrycia przez zautomatyzowany system czegoś, co powinno zostać zweryfikowane przez człowieka, generowane jest powiadomienie (czasami nazywany „wykroczeniem"), a w niektórych przypadkach może następować automatyczna reakcja polegająca na zablokowaniu dostępu lub wyłączeniu komponentu. Powiadomienia mogą być generowane na podstawie określonych zdarzeń, korelacji zachodzących zdarzeń lub po osiągnięciu określonych progów.

Sztuka analizowania logów skupia się właśnie na tych obszarach. Jeśli system jest dostrojony z taką czułością, że zespół do spraw bezpieczeństwa stale będzie otrzymywał fałszywe powiadomienia, to wszystkie powiadomienia zostaną szybko zignorowane. Z drugiej strony, jeśli niektóre powiadomienia nie będą otrzymywane co najmniej regularnie, najprawdopodobniej będą pomijane pewne rzeczy, na które powinno się zwrócić uwagę. Każdy rodzaj fałszywego powiadomienia wymaga pętli sprzężenia zwrotnego, tak aby ustalić, czy sensowne jest odfiltrowywanie tego rodzaju zdarzeń, podniesienie progów lub podjęcie innych działań w celu zmniejszenia liczby fałszywych powiadomień. Należy także zastanowić się nad uruchomianiem okresowych testów, w wyniku których zostaną wygenerowane powiadomienia, a następnie upewnić się, że nie zostaną one zignorowane.

Istnieją pewne powiadomienia, które prawie zawsze należy monitorować. Liczne nieudane logowania dla uprzywilejowanych użytkowników, złośliwe oprogramowanie wykryte w systemach oraz inne powiadomienia, które mogą być prekursorami incydentów bezpieczeństwa, powinny być sprawdzone, nawet jeśli byłyby to zwykle fałszywe alarmy.

Nie należy zapominać, że konieczne jest także otrzymywanie powiadomień w momencie, gdy dzienniki przestaną być tworzone. Jest to także problem związany z bezpieczeństwem! W wielu przypadkach może to po prostu wskazywać na nieprawidłowe działanie pewnego komponentu, co z kolei może uniemożliwić dostrzeżenie problemu w przyszłości. W niektórych przypadkach może to jednak wskazywać na trwający atak.

Zasadniczo zautomatyzowane reagowanie może wydawać się świetnym pomysłem, aczkolwiek tak naprawdę może zakłócać funkcjonowanie firmy. Oprócz awarii spowodowanych niepoprawną odpowiedzią lub nadmierną automatyczną reakcją, systemy automatycznej reakcji mogą zostać wykorzystane przez atakujących do spowodowania awarii.

Może to wcale nie być zabawne, gdy zostanie wydana znaczna suma pieniędzy z myślą o zapobieganiu atakom typu DDoS, a jedyne, co zostanie osiągnięte, to umyślne umożliwienie atakującym przeprowadzenia łatwego ataku typu DDoS za pomocą prostego skanera portów lub kilku nieudanych prób logowania. Niektóre środowiska mają tak wysokie wymagania bezpieczeństwa, że bardziej akceptowalna jest możliwość wystąpienia awarii systemu niż nawet niewielkie ryzyko wystąpienia ataku kontynuowanego aż do momentu zbadania go przez człowieka. Niemniej jednak w większości przypadków ryzyko operacyjne i bezpieczeństwo powinny być ściślej zrównoważone.

Alarmowanie nie powinno być działaniem typu „włącz i zapomnij". Często potrzebny jest sposób na rotowanie udziału różnych osób, tak aby ktoś był przez cały czas w pogotowiu,

oraz na upewnienie się, że powiadomienie zostanie potwierdzone w określonym czasie lub przekazane komuś innemu. W środowisku w chmurze dostępnych jest wiele wszechstronnych usług i alarmowanie nie jest tu wyjątkiem. W większości przypadków ten sam system może być wykorzystywany zarówno do reakcji operacyjnych, jak i działań związanych z reakcjami bezpieczeństwa.

W przypadku większych organizacji system alarmowania jest zwykle budowany samodzielnie. Ewentualnie zawierana jest umowa z dostawcą zarządzanych usług bezpieczeństwa (MSSP, ang. *Managed Security Service Provider*) na utworzenie centrum operacyjnego bezpieczeństwa 24x7 (SOC, ang. *Security Operations Center*), w celu monitorowania i reagowania na powiadomienia. Pomieszczenie z dużą liczbą ekranów wyświetlających ważne grafiki jest jedynie opcjonalne, aczkolwiek może robić wrażenie na kadrze zarządzającej i klientach oraz może pomóc w szybkim przedstawieniu ważnych informacji w pilnej sytuacji. W wielu przypadkach w organizacjach wykorzystywany jest model hybrydowy, w którym część monitorowania i ostrzegania na niższym poziomie jest wykonywana przez MSSP, natomiast ważniejsze powiadomienia są przekazywane personelowi wewnętrznemu.

W przypadku nowoczesnych systemów mogą być generowane miliardy zdarzeń w dziennikach. Możliwe jest wtedy wykorzystanie jeszcze większej automatyzacji, tak aby sobie z nimi poradzić – w takiej sytuacji bardzo przydatny może być SIEM.

Informacje o bezpieczeństwie i menedżerowie zdarzeń

Menedżer zdarzeń i informacji o bezpieczeństwie (SIEM, ang. *Security Information and Event Manager*) może zostać wykorzystany do wykonania niektórych lub wszystkich kroków, które zostały opisane w poprzednich sekcjach. Na przykład możliwe jest posiadanie dzienników agregacji SIEM lub zamiast tego osobnych dzienników agregacji i filtrowania, z których tylko część jest wysyłana do SIEM. Wielu dostawców usług w chmurze oferuje tanie, wysokonakładowe usługi agregacji dzienników, które oprócz wykrywania i reagowania na zdarzenia związane z bezpieczeństwem są często wykorzystywane do rozwiązywania problemów operacyjnych. Z tego powodu w wielu organizacjach wykorzystywany jest agregator dzienników w chmurze do przekazywania zdarzeń związanych z bezpieczeństwem do SIEM.

Reguły SIEM mogą być wykorzystywane do wykrywania potencjalnego nieprawidłowego zachowania przez korelowanie zdarzeń, które nastąpiły w dwóch różnych miejscach lub przez porównywanie danych aktualnych i historycznych. Poniżej przedstawiono kilka pytań, które mogą zostać postawione przez odpowiednio skonfigurowany SIEM lub przez operatora bezpieczeństwa przeglądającego powiadomienia SIEM:

- „Ruch w bazie danych jest o 200% wyższy niż średnia miesięczna. Może aplikacja jest teraz bardzo popularna, ale czy przypadkiem ktoś systematycznie nie kradnie danych?"
- „Właśnie zauważono połączenie wychodzące z adresem IP, który był ostatnio używany przez znaną osobę atakującą, zgodnie z kanałem informacyjnym dotyczącym zagrożeń. Czy to zaatakowany system komunikuje się z serwerem zarządzającym C&C (ang. *Command and Control*)?"

- „Wykonano 150 nieudanych prób logowania na koncie, które następnie zakończyły się powodzeniem. Czy to udany atak typu „brute force"?
- „Zauważono pojedynczą nieudaną próbę logowania na 300 różnych kontach, a następnie poprawne logowanie na konto numer 301. Czy to udany atak z użyciem hasła?"
- „Po skanowaniu portów nastąpił duży ruch z portu, który nie był używany od miesięcy. Skanowanie portów odbywa się przez cały czas, ale być może została znaleziona i narażona na atak usługa?"
- „John zwykle nie loguje się o 3:00 lub z tego kraju. Może to tak naprawdę nie jest John?"
- „Trzy różne konta zalogowane z tego samego systemu w ciągu 30 minut. Wydaje się mało prawdopodobne, że wszyscy ci ludzie faktycznie korzystają z tego systemu, więc może system i konta są zagrożone?"
- „Nowe konto administracyjne zostało właśnie utworzone poza normalnymi godzinami pracy. Może ktoś pracuje do późna, ale może jest jakiś problem?"
- „Ktoś właśnie został dodany do grupy administratorów. To rzadkie wydarzenie, więc czy nie powinniśmy tego sprawdzić?"
- „Dlaczego zapora ogniowa zaprzecza, że źródłem jest system wewnętrzny? Albo coś jest źle skonfigurowane, albo nieuprawniony użytkownik próbuje poruszać się po sieci".

SIEM może być uruchamiany wewnętrznie jako część SOC lub może być zarządzany przez dostawcę usług bezpieczeństwa w imieniu klienta. Niezależnie od tego, czy SIEM jest użytkowany, czy nie, należy się upewnić, że zostały spełnione wymagania dotyczące agregacji i przechowywania, analizowania, wyszukiwania i korelacji, ostrzegania i możliwości automatycznej reakcji.

Używać SIEM, czy nie używać SIEM?

Czy istnieje potrzeba posiadania informacji o bezpieczeństwie oraz menedżera zdarzeń? Mniejsze organizacje są w stanie poradzić sobie, wykorzystując funkcję agregacji dzienników do generowania prostych powiadomień lub pracowników przeszukujących dzienniki w poszukiwaniu zagrożeń. Dedykowane produkty SIEM są dostępne nie bez powodu. Logika i reguły wymagane do wyciągania odpowiednich danych z dzienników w wielu różnych formatach, korelowanie dzienników z różnych źródeł, posiadanie wiedzy o tym, jak przebiega typowy atak oraz uzyskiwania informacji na temat bieżących ataków na całym świecie mogą być bardzo skomplikowane. Całą tę pracę trudno jest powielić wewnętrznie, tak więc w wielu większych środowiskach wykorzystuje się produkty SIEM albo wynajmuje zarządzaną usługę bezpieczeństwa do obsługi SIEM.

Threat Hunting

Dopiero po zapoznaniu się z podstawami dotyczącymi: zbierania dzienników i mierników związanych z bezpieczeństwem, ich analizowania oraz reagowania na powiadomienia generowane przez systemy, należy przejść do polowania na zagrożenia.

Polowanie na zagrożenia polega na szukaniu problemów zamiast na śledzeniu określonych powiadomień. Postępowanie zaczyna się od postawienia hipotezy, takiej jak: „Być może jestem atakowany przez Advanced Persistent Threat 12345" lub „Może ktoś szuka tajnych planów mojego statku kosmicznego". Następnie poszukuje się dowodów, które pozwolą potwierdzić lub obalić taką hipotezę.

Przygotowanie do incydentu

W momencie, gdy już się ma użyteczne dzienniki, które są wykorzystywane do otrzymywania powiadomień, konieczne jest zaplanowanie, co zrobić, gdy jedno z powiadomień okaże się prawdziwe. W zależności od ryzyka dla środowiska plany nie muszą być wyczerpujące, ponieważ nawet częściowe planowanie może być bardzo pomocne.

Pierwsza decyzja, którą należy podjąć, dotyczy określenia momentu, w którym wezwana zostanie pomoc z zewnątrz. W dużej mierze zależy to od postrzeganego ryzyka dla organizacji, powagi incydentu oraz wielkości zespołu do spraw bezpieczeństwa. Nawet duże, dobrze przygotowane organizacje mogą potrzebować pomocy z zewnątrz w przypadku poważniejszych incydentów bezpieczeństwa. Można szybko wyszukać wiele firm specjalizujących się w reagowaniu na incydenty i dobrym pomysłem jest uprzednie sprawdzenie dwóch z nich na wypadek, gdyby były potrzebne.

Ponadto można rozważyć ubezpieczenie w zakresie bezpieczeństwa cybernetycznego, szczególnie jeśli posiadany zespół jest niewielki, a reagowanie na incydenty może być wykonane we własnym zakresie. W niektórych przypadkach ubezpieczenie to może być uwzględnione w ogólnych polisach ochrony biznesu, chociaż wiele z nich wyklucza incydenty związane z cyberbezpieczeństwem. Podobnie jak w przypadku każdego ubezpieczenia, należy uważnie przeczytać zakres i wykluczenia, ponieważ niektóre polisy wykluczają typowe ataki, takie jak ataki socjotechniczne, lub odmawiają wypłaty odszkodowania na podstawie niejasnych wymagań bezpieczeństwa dla ubezpieczonego. Jednakże ubezpieczenia tego typu mogą być wystarczające do pokrycia większości lub wszystkich wydatków związanych z reakcją na incydent.

Najważniejsze prace przygotowawcze dotyczą gromadzenia i przechowywania omówionych już dzienników, tak aby można było przywołać rozsądną ilość aktualnych i historycznych danych do przeprowadzenia dochodzenia. Oprócz tego konieczne jest zebranie zespołu, sporządzenie planu i przygotowanie niektórych narzędzi.

Zespół

Stresujące zadanie zespołu reagowania na incydenty polega na zdobyciu wiedzy na temat tego, co wydarzyło się podczas ataku i jak najlepiej ograniczyć taki incydent. Pierwszą

rzeczą, która musi zostać zrobiona, jest zidentyfikowanie głównych i rezerwowych liderów reagowania na incydenty techniczne. Osoby te powinny być odpowiedzialne za prowadzenie wszelkich wewnętrznych dochodzeń oraz koordynację z pomocą zewnętrzną.

Konieczne jest także zidentyfikowanie głównych i rezerwowych liderów biznesowych, którzy powinni być natychmiast dostępni, w celu autoryzowania decyzji biznesowych, takich jak wycofanie systemów lub autoryzacja płatności. W mniejszych organizacjach liderem technicznym i biznesowym mogą być te same osoby, aczkolwiek nadal jest wymagane posiadanie co najmniej jednej osoby podstawowej i jednej osoby rezerwowej.

Oprócz kierownictwa zespołu potrzebni są także specjaliści techniczni z obszarów, które najprawdopodobniej mogą zostać zaatakowane według używanego modelu zagrożenia. Na przykład, jeśli istnieje obawa o kradzież danych klientów z aplikacji internetowej w chmurze, być może konieczne jest wykorzystanie specjalistów do spraw sieci, serwerów www, baz danych oraz specjalistów zaznajomionych z wewnętrznym projektem i działaniem samej aplikacji. Niepożądana jest sytuacja, aby w trakcie incydentu uświadomić sobie, że nie ma możliwości dotarcia do jakiejkolwiek osoby znającej komponent, którego dotyczy incydent.

Na koniec, potrzebne są również niżej wymienione kontakty podstawowe oraz zapasowe:

- Dział prawny lub osoba z firmy prawniczej, aby pomóc w pytaniach dotyczących przestrzegania umów i przepisów.
- Dział komunikacji lub osoba upoważniona do rozmowy z mediami i organami ścigania, jeśli to konieczne.
- Dział HR lub osoba upoważniona do podejmowania decyzji o zatrudnieniu/zwalnianiu pracowników w przypadku zidentyfikowania zagrożenia wewnętrznego.

Wszystkie wymienione obowiązki mogą spoczywać na różnych osobach lub mogą być wykonywane przez wcześniej zidentyfikowanych liderów, pod warunkiem, że określony został skład podstawowy i rezerwowy dla każdego obszaru.

Niezależnie od tego, czy zespół reagowania na incydenty jest dostępny w pełnym wymiarze godzin, czy nie, powinno się dysponować również odpowiednikiem ochotniczej straży pożarnej. Należy zidentyfikować osoby posiadające wiedzę, które można przeszkolić w zakresie reagowania na incydenty. Osoby takie powinny mieć wstępną zgodę kierownictwa na porzucenie swoich dotychczasowych obowiązków na rzecz działań związanych z incydentem o wysokim priorytecie.

Poniżej zamieszczono kilka innych uwag dotyczących tworzenia i utrzymywania zespołu reagowania na incydenty:

- Nikt nie chce pełnić dyżuru podczas weekendu lub wakacji. Niestety wiedzą o tym osoby atakujące, tak więc istnieje duże prawdopodobieństwo wystąpienia incydentu w tych niewygodnych momentach.

- Jeśli w organizacji reakcja na incydent zdarza się regularnie, rutyna może stanowić poważny problem. Może to być szczególnie niepokojące w przypadku zespołów złożonych z ochotników, którzy oprócz zadania związanego z opanowaniem incydentu są obciążeni swoją zwykłą pracą. Jeśli to możliwe, należy rotować członków zespołu, aby mieli przerwę od działań związanych z reagowaniem na incydenty.
- Należy z wyprzedzeniem określić ogólne role członków zespołu w reagowaniu na incydenty i sporządzić listę, tak aby podczas incydentu nikt nie był zdezorientowany brakiem wiedzy, za co jest odpowiedzialny.
- Należy urządzać spotkania zespołu co najmniej raz na kwartał, aby upewnić się, że wszyscy są nadal zapoznani z planami.

W momencie, gdy już zorganizowano zespół reagowania na incydenty, konieczne jest jeszcze określenie planów, które taki zespół musi wykonać.

Plany

Większość porad dotyczących składu zespołu, które zostały omówione w poprzedniej części nie jest charakterystyczna dla środowiska w chmurze, poniżej omówiono natomiast plany specyficzne dla chmury. Konieczne jest określenie kilku prawdopodobnych scenariuszy dla środowiska w chmurze i zapewnienie planów ich pokrycia.

W ramach planowania konieczne jest zrozumienie, co zrobi dostawca usług w chmurze w przypadku naruszenia bezpieczeństwa. Czy do jego obowiązków należy przekazanie dodatkowych dzienników lub zrobienie zdjęć kryminalistycznych? Czy zostaną podane informacje kontaktowe na temat incydentów związanych z bezpieczeństwem? Jest bardzo niepożądane, aby w trakcie incydentu w celu dowiedzenia się, jaki jest zakres odpowiedzialności dostawcy, konieczne było zapoznanie się z warunkami korzystania z usługi.

W wielu przypadkach dostawca usług w chmurze ponosi odpowiedzialność za reagowanie na incydenty związane z naruszeniem jego usług w chmurze, ale już nie za incydenty, które dotyczą wyłącznie aplikacji klienta. Istnieją jednak wyjątki, takie jak ataki DDoS, w których dostawca usług w chmurze może współpracować z klientem w celu złagodzenia ataku lub może wyłączyć dostęp sieci zewnętrznej do aplikacji, tak aby atak nie miał wpływu na innych klientów! Istotne jest, aby zawczasu posiadać wiedzę, co dostawca usług w chmurze jest w stanie zrobić dla klienta w przypadku ataku.

Istotne jest także zapewnienie co najmniej niewielkiego, wstępnie zatwierdzonego budżetu z przeznaczeniem na rozwiązywanie problemów związanych z bezpieczeństwem. Powinien być on wystarczający do pokrycia rozsądnych i uzasadnionych wydatków, bez konieczności przechodzenia potencjalnie długiego procesu zakupu i zatwierdzania. Na przykład, jeśli częścią planu jest skorzystanie z usług firmy reagującej na incydent, to należy zapewnić pokrycie kosztów, co najmniej wstępnej opłaty za takie konsultacje. W przypadku gdy część planu obejmuje natychmiastowe wysłanie pracowników samolotem, należy wcześniej zarezerwować potrzebne bilety lotnicze. Należy starać się planować

budżet i wstępnie zatwierdzać wszystkie koszty, które najprawdopodobniej będą potrzebne w ciągu pierwszych kilku godzin po wystąpieniu incydentu.

Bardzo ważną częścią planowania reagowania na incydenty jest ustalanie priorytetów. Nie ma potrzeby reagować w taki sam sposób na próbę ataku i na aktywną kradzież danych. Należy utworzyć co najmniej kilka poziomów istotności dla incydentów bezpieczeństwa z pewnymi wskazówkami, co robić w każdym przypadku. Na przykład możliwe jest wymienienie kategorii dla „potwierdzonego nieudanego ataku", „potwierdzonego udanego ataku bez utraty danych" i „potwierdzonego udanego ataku z utratą danych". Należy też pamiętać, że może być wymagana zupełnie inna reakcja w momencie, gdy incydenty zwiększają skalę.

Powinno się także określić wytyczne dla całej organizacji, dotyczące zgłaszania podejrzeń możliwości wystąpienia incydentów bezpieczeństwa oraz niezakłócania procesu dochodzenia. Wytyczne takie mogą zostać sprecyzowane w prosty sposób w podręczniku dla pracownika, na przykład: „Jeśli podejrzewasz, że nieautoryzowany użytkownik uzyskuje dostęp do naszych systemów informatycznych, zadzwoń pod następujący numer, aby zgłosić podejrzenie naruszenia bezpieczeństwa. Jesteś uprawniony do zamknięcia zaatakowanych, niepotrzebnych systemów, ale nie jesteś uprawniony do usuwania jakichkolwiek systemów, kasowania jakichkolwiek danych ani do podejmowania prób odwetowych".

W przypadku gdy nie zaistniała jeszcze okazja do przetestowania przygotowanych planów, należy rozważyć wykonanie ćwiczeń. Możliwe jest przeprowadzenie takich ćwiczeń wewnętrznie, wymyślając wiarygodny scenariusz wydarzeń albo w specjalnym środowisku testowym. Możliwe jest także skorzystanie z usług firm, które to ułatwiają, udostępniając scenariusze, fałszywe biuletyny informacyjne oraz inne rekwizyty pomocne w pomyślnym przeprowadzeniu ćwiczeń. Dodatkowo firmy te mogą udzielić krytycznych rad odnoszących się do wykonania planu w celu wyeliminowania słabości. Na przykład prawdopodobnym scenariuszem może być atak w toku, gdzie wymaganą reakcją jest przejście do trybu blokady. W środowisku w chmurze może obejmować to jedną lub więcej z poniższych czynności:

- Plan wyłączenia całego dostępu do portali w chmurze i interfejsów API innych niż minimum wymagane podczas incydentu. Na przykład przy założeniu, że tylko cztery osoby potrzebują dostępu w krótkim okresie, możliwe jest zainstalowanie skryptów, w celu wyłączenia dostępu wszystkim innym użytkownikom.
- Plan wyłączenia wszelkiego dostępu sieciowego do środowiska w chmurze lub jego części. Możliwe jest całkowite wyłączenie aplikacji lub tymczasowe wyłączenie niektórych z jej funkcjonalności.
- Plan zamknięcia całego środowiska, zablokowania serwera sekretów i odtworzenia nowego środowiska.

Część planu powinna obejmować tworzenie kopii zapasowych, których można użyć do przywrócenia danych i funkcjonalności. *Należy upewnić się, że kopie zapasowe znajdują się na koncie odseparowanym od danych produkcyjnych, z oddzielnymi administracyjnymi danymi uwierzytelniającymi*. Do tej pory udokumentowano (*https://www.infoworld.com/article/2608076/data-center/murder-in-the-amazon-cloud.html*) przypadki ataków, podczas których zostały skasowane nie tylko dane produkcyjne, ale także wszystkie kopie zapasowe, które były dostępne z konta produkcyjnego.

Ważne jest, aby zrozumieć, jak długo może potrwać proces przywracania. Często opracowana jest całkowicie rozsądna strategia odzyskiwania, z tym że jest ona bardzo czasochłonna. Nie ma potrzeby, aby organizacja była w stanie funkcjonować w 100% podczas procesu odzyskiwania. Całkowicie rozsądne mogą być opóźnienia w wysyłaniu rachunków lub odręczne zapisywanie notatek w celu późniejszego wpisania ich do systemów IT, muszą zostać zachowane jedynie podstawowe funkcje biznesowe.

Narzędzia

Podczas opracowywania planów należy zwrócić uwagę na to, że konieczne jest wyposażenie zespołu do spraw reagowania na incydenty w narzędzia niezbędne do wdrożenia planu. W przypadku tradycyjnego środowiska lokalnego takie narzędzia to najczęściej zwykłe torby, zawierające laptopy, kable i podobne materiały (wspomniane wcześniej „torby podręczne"). W przypadku środowiska w chmurze oferowane są wirtualne odpowiedniki niektórych z tych narzędzi.

W pewnym stopniu dobór narzędzi zależy od tego, jak wygląda używane środowisko oraz co występuje w ofercie dostawcy usług w chmurze, aczkolwiek zespół powinien mieć do dyspozycji przynajmniej wirtualne obrazy zawierające narzędzia analizy kryminalistycznej oraz konto w chmurze do stworzenia infrastruktury kryminalistycznej. Zazwyczaj, jeśli na koncie w chmurze nie jest nic przechowywane, to nie wiąże się to z jakimikolwiek opłatami, dlatego należy zachować osobne konto w chmurze na wypadek reagowania na incydenty, które może zostać połączone z kontem produkcyjnym. Niektórzy dostawcy usług w chmurze oferują również dokumentację dotyczącą przeprowadzania dochodzeń i cyfrowych analiz kryminalistycznych w swoich środowiskach, która może wskazywać na określone narzędzia.

Należy opracować szczegółowe, *przetestowane* procedury dla najczęstszych zadań reagowania na incydenty. Na przykład może być potrzebna procedura zbierania informacji kryminalistycznych z pamięci i dysków maszyny wirtualnej z systemem Linux w środowisku w chmurze. Taka procedura powinna zawierać dokładne polecenia, takie jak: uruchomienie LiME w celu przechwycenia zrzutu pamięci, wygenerowanie skrótu

zrzutu, weryfikacja zrzutu za pomocą Volatility, wykonanie twardego resetu zainfekowanego komputera w celu uniemożliwienia złośliwym programom zatarcia śladów przed ponownym uruchomieniem komputera oraz wykonanie migawek dysków.

Poniżej przedstawiono kilka innych narzędzi, które mogą być pomocne:

- Zorientowane na chmurę narzędzia analizy kryminalistycznej, które mogą być pomocne w zrozumieniu, co wydarzyło się w danym systemie.
- Aktualne diagramy przedstawiające konfigurację sieci, lokalizacje danych i lokalizacje rejestratorów zdarzeń.
- Testowane systemy łączności. Czy będzie istniała możliwość odpowiedzi na zagrożenie, jeśli platforma komunikatora, poczta e-mail lub systemy telefoniczne zostaną wyłączone? W nagłych wypadkach pracownicy mogą mieć zezwolenie na używanie osobistych wiadomości e-mail i telefonów komórkowych do wykonywania pracy, nawet jeśli jest to zwykle niedozwolone. Zalecane jest przemyślenie takich decyzji z wyprzedzeniem.
- Listy kontaktów zarówno do osób wewnętrznych, jak i zewnętrznych, takich jak dostawcy usług w chmurze, firmy reagujące na incydenty lub inni dostawcy, którzy mogą brać udział w reagowaniu na incydenty.
- Kwatera główna. W środowisku w chmurze w większości przypadków nie ma fizycznego kontaktu ze sprzętem, aczkolwiek nadal potrzebne jest fizyczne lub wirtualne pomieszczenie, w którym zespół może się spotykać, wymieniać informacje i podejmować decyzje. W przypadku gdy przewidziani są także uczestnicy zdalni, należy zapewnić sensowne sposoby uczestnictwa, takie jak udostępnianie ekranu i rozsądny system audio.
- Listy kontrolne. Nie zawsze należy być fanem list kontrolnych bezpieczeństwa, na których zaznaczone jest posiadanie zapory sieciowej, oprogramowania antywirusowego oraz podobnych elementów, bez zweryfikowania skuteczności tych elementów. Jednakże reakcja na incydent jest często wykonywana przez spanikowanych i zmęczonych ludzi. W takich sytuacjach listy kontrolne, pomocne w realizacji planów, są niezbędne do upewnienia się, że nie pominięto czegokolwiek naprawdę ważnego. Na przykład w jednej liście kontrolnej online (*https://zeltser.com/security-incident-log-review-checklist/*) może być zawarty sugerowany, przydatny zestaw dzienników, który należy przejrzeć w przypadku wystąpienia incydentu.
- Formularze do dokumentowania działań związanych z reagowaniem na incydenty. Na przykład w ofercie instytutu SANS występują niektóre formularze (*https://www.sans.org/score/incident-forms*), które mogą zostać dostosowane do potrzeb organizacji.
- Oprogramowanie do reagowania na incydenty, zawierające komponenty przeznaczone do śledzenia incydentów oraz wbudowane podręczniki reagowania na incydenty.

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

powiadomienia o złośliwych kampaniach. W przypadku gdy obserwowane jest podejrzane zachowanie oraz zostało opublikowane ostrzeżenie informujące o tym, że dana branża jest atakowana przez konkretne podmioty wykorzystujące określone taktyki, techniki i procedury, to informacje takie mogą być pomocne w zorientowaniu się w sytuacji.

3. W fazie *decyzyjnej* należy wybrać następną taktykę, która zostanie wykorzystana w celu zminimalizowania szkód lub umożliwienia powrotu do stanu pierwotnego. Na przykład można zdecydować o przełączeniu niektórych systemów w tryb offline, cofnięciu dostępu, poddaniu kwarantannie systemów lub zbudowaniu nowego środowiska.
4. W fazie *reakcji* zawiera się faktyczne zastosowanie wybranej taktyki. W tym przypadku korzystanie z infrastruktury w chmurze może być naprawdę pomocne, szczególnie jeśli zainwestowano w powtarzalne metody budowania środowisk w chmurze zamiast ich organicznego wzrostu w czasie. Oto kilka przykładów:
    - Większość środowisk w chmurze ma wyraźniej oddzieloną infrastrukturę obliczeniową od pamięć masowej niż środowiska tradycyjne. Utrzymanie nieautoryzowanego dostępu przez modyfikację zawartości w magazynach danych jest dla atakujących o wiele trudniejsze, aczkolwiek nie jest niemożliwe. Każda instancja infrastruktury obliczeniowej zawiera tysiące plików wykonywalnych i wpisów konfiguracji, ale zwykle można je znacznie łatwiej odbudować niż dane. Biorąc pod uwagę ten podział, można zastosować poprawki obrazów w celu zamknięcia luki, która umożliwiła osobie atakującej włamanie się. Następnie można zamknąć wszystkie instancje obliczeniowe, zastąpić je poprawionymi i powtórnie połączyć je z magazynami danych, przy zachowaniu minimalnego przestoju.
    - Możliwe jest także łatwe poddawanie systemów kwarantannie, używając w tym celu skryptów do wywoływania API, które zablokują grupy zabezpieczeń lub sieciowe listy ACL. W tradycyjnym środowisku, aby uzyskać ten sam efekt, może być konieczne ręczne zalogowanie się do wielu różnych routerów i zapór sieciowych lub odłączenie kabli.

Po wykonaniu wszystkich czynności pętla zaczyna się od nowa. Należy obserwować reakcję osoby atakującej na podjęte działania i następnie ponownie przejść przez etapy orientacji, decydowania i podjęcia ponownych działań. Pętle takie powinny być względnie szybkie i trwać do momentu, gdy obserwacje wykażą, że incydent został zażegnany.

Należy pamiętać, że praktycznie nigdy nie można być wystarczająco przygotowanym. Każdy incydent wprowadza bałagan, nawet w przypadku naprawdę dobrego przygotowania się na niego. Warto czasem poświęcić 15 sekund na sporządzenie notatek na temat zdobytej wiedzy, zanim przejdzie się do dalszych działań, ponieważ później może to być trudne do zapamiętania.

Nie należy obawiać się kontaktu z firmą zajmującą się reagowaniem na incydenty w przypadku, gdy sytuacja wymyka się spod kontroli lub nie czynione są postępy. Większość atakujących ma więcej doświadczenia w atakowaniu niż obrońcy!

Forensic w chmurze

Tytuł ten może przyciągać na myśl obrazy programu telewizyjnego CSI, ale niestety rzeczywistość jest nieco mniej ekscytująca. Zasadniczo celem jest po prostu skopiowanie wszystkiego, co może być ważne, a następnie wykorzystanie narzędzi do analizy takiego skopiowanego obrazu.

Ważne jest, aby wykonywać kopie w udokumentowany, powtarzalny sposób, tak aby zawsze można było wykazać posiadanie dobrej kopii oryginalnych danych, które nie zostały zmienione. Zwykle wiąże się to z wygenerowaniem ciągu weryfikacyjnego (skrótu kryptograficznego), który można wykorzystać do wykazania, że jest to kopia nieuszkodzonych danych. Skrót kryptograficzny, taki jak SHA-256, został zaprojektowany w taki sposób, aby był szybki do obliczenia, i jednocześnie było praktycznie niemożliwe utworzenie kolejnego fragmentu danych, który będzie miał ten sam skrót. Wykorzystując kopię danych oraz skrót kryptograficzny, każdy może szybko wygenerować skrót i porównać go z oryginałem, aby upewnić się, że jego kopia jest taka sama jak ta, którą zebrał pierwotny śledczy. Ponadto nikt nie może umyślnie lub przypadkowo dokonać zmian danych, które w razie czego są łatwe do wykrycia. Oczywiście, można również zapisać oryginalną kopię na nośnikach tylko do odczytu i za każdym razem dokonywać porównań kopii bit po bicie, byłoby to jednak o wiele bardziej czasochłonne!

W przykładowej procedurze przedstawionej w podrozdziale „Narzędzia" na stronie 165 zawarto opis jednego ze sposobów uzyskania obrazów pamięci maszyny wirtualnej i dysków, aczkolwiek podczas dochodzenia mogą być potrzebne inne artefakty kryminalistyczne. Na przykład może być zamierzone wykonanie migawek lub kopii zapasowych baz danych, tak aby porównać i sprawdzić, czy atakujący dokonał jakichkolwiek zmian w bazie danych. Może być także pożądane przeanalizowanie przechwyconych pakietów sieciowych w celu sprawdzenia, co osoba atakująca lub złośliwe oprogramowanie robiło w sieci.

Blokada nieautoryzowanego dostępu

Może to wydawać się oczywiste, ale często jest trudniejsze, niż się wydaje, szczególnie jeśli atakujący jest w systemie od jakiegoś czasu i ma dostęp administracyjny. W takiej sytuacji korzystne jest wdrożenie zaleceń, które zostały przedstawione w rozdziale 6, dotyczących segmentacji sieci, dzięki czemu atak może zostać ograniczony do określonej części sieci.

Częstą reakcją w takim przypadku jest także resetowanie haseł oraz kluczy API wszystkich użytkowników (w tym automatyzacji), co może zakłócać normalne operacje, blokując przychodzący i wychodzący dostęp do sieci.

Powinno się mieć przygotowane narzędzia oraz procesy, które mogą zostać wykorzystane do jednoczesnego, szybkiego blokowania całego dostępu.

Zatrzymywanie ekstrakcji danych oraz komunikacji z serwerami C&C

Jeżeli komunikacja sieciowa nie została zamknięta w ramach blokowania nieautoryzowanego dostępu, może być konieczne zamknięcie komunikacji wychodzącej w celu zatrzymania połączeń osób atakujących z serwerami dowodzenia i kontroli lub zatrzymania ciągłej utraty danych.

Odzyskiwanie

Kolejnym krokiem po pomyślnym odkryciu i zatrzymaniu ataku jest zaprowadzenie porządku i upewnienie się, że nie ma już żadnych sposobów na powrót atakujących do systemu.

Ponowne instalowanie systemów informatycznych

Zdecydowanie najprostszym i najskuteczniejszym sposobem odzyskiwania z punktu widzenia IT jest ponowne wdrożenie wszystkich systemów, których dotyczy problem. Ponownie jest to trochę łatwiejsze w chmurze, ponieważ nie istnieje konieczność nabywania nowego fizycznego sprzętu, gdyż to dostawca chmury jest odpowiedzialny za zapewnienie pojemności. Wszelkie zagrożone systemy w chmurze należy odtworzyć, a ruch produkcyjny należy przenieść na nowe systemy. Wszelkie dotknięte stacje robocze należy usunąć i odtworzyć ze znanych, dobrych obrazów. Można przypomnieć nieśmiertelne słowa Ellen Ripley z filmu *Alien*: „Zrzucić z orbity głowice atomowe na całe miejsce. To jedyny sposób, by mieć pewność."

Jeśli nie jest to możliwe, konieczna jest akceptacja znacznego ryzyka związanego z dalszym użytkowaniem systemów, nad którymi pewna osoba atakująca miała w przeszłości kontrolę. Oczywiście można uruchamiać skanery złośliwego oprogramowania, utrzymywać dodatkowe karty w sieci i procesy jako mierniki naruszenia bezpieczeństwa oraz wprowadzać inne środki bezpieczeństwa, niemniej zmiana pojedynczego wpisu w rejestrze lub jeden pominięty element złośliwego oprogramowania może wystarczyć do ponownego przejęcia przez osobę atakującą.

Powiadomienia

Z niektórych regulacji i umów może wynikać obowiązek powiadamiania klientów lub zgłaszania naruszenia organom ścigania.

Zalecane jest powiadamianie opinii publicznej, nawet jeśli nie istnieje taki obowiązek, ponieważ może to być pomocne w ograniczeniu negatywnych skutków dla wizerunku firmy, jeśli wiadomość w końcu wyjdzie na jaw. Z oczywistych względów nie istnieją wiarygodne dane na temat liczby udanych aktów zatuszowania ataku, aczkolwiek dobrze są znane ataki na Yahoo!, Cathay Pacific oraz inne firmy, których nie udało się ukryć przed opinią publiczną.

Zdobyta wiedza

Jak najszybciej po zakończonym incydencie należy przeanalizować go i wyciągnąć wnioski, na podstawie których należy wprowadzić wszelkie konieczne zmiany w składzie zespołu, planach, procedurach, narzędziach i listach kontrolnych, które mogą być pomocne następnym razem. Zalecane jest, aby podczas incydentu sporządzać notatki, które później mogą zostać wykorzystane do tego celu.

Budowa całego zespołu oraz opracowanie procesu reagowania na incydenty jest bardzo skomplikowaną sprawą. Mimo że omówione zostały najbardziej istotne punkty dla środowisk w chmurze, to zalecane jest zapoznanie się z przewodnikami: Insider's Guide to Incident Response (*https://www.alienvault.com/resource-center/ebook/insider-guide-to-incident-response*) oraz NIST SP 800-61 (*https://csrc.nist.gov/publications/detail/sp/800-61/rew-2/final*).

Przykładowe mierniki

Podobnie jak w przypadku innych procesów biznesowych, trudno jest ustalić, czy czynione są postępy, jeśli nie istnieje możliwość podania niektórych mierników w zakresie wykrywania, reagowania i odzyskiwania.

Poniżej zamieszczono kilka przykładowych mierników, których użycie warto rozważyć:

Wykrycia
: Liczba zdarzeń w miesiącu, miesięczna liczba powiadomień, odsetek powiadomień potwierdzonych incydentami, odsetek powiadomień fałszywie pozytywnych.

Czas reakcji
: Czas, jaki upłynął od momentu wystąpienia powiadomienia do jego zrewidowania, czas, jaki upłynął od momentu rozpoczęcia potwierdzonego incydentu do jego zamknięcia.

Odzyskiwanie
: Czas wymagany do ponownego wdrożenia systemów, których dotyczy problem.

Miernik ogólny
: Szacunkowy koszt każdego incydentu, w tym czas, wydatki i szkody wizerunkowe.

Przykładowe narzędzia do wykrywania, reagowania i odzyskiwania

Poniżej przedstawiono listę niektórych reprezentatywnych rozwiązań w obszarze wykrywania, reagowania i odzyskiwania w chmurze. Podobnie jak w rozdziale 5, umieszczenie lub niezamieszczenie narzędzia na liście nie jest równoznaczne z tym, że jest ono polecane lub niepolecane. Są to tylko przykłady różnych popularnych narzędzi:

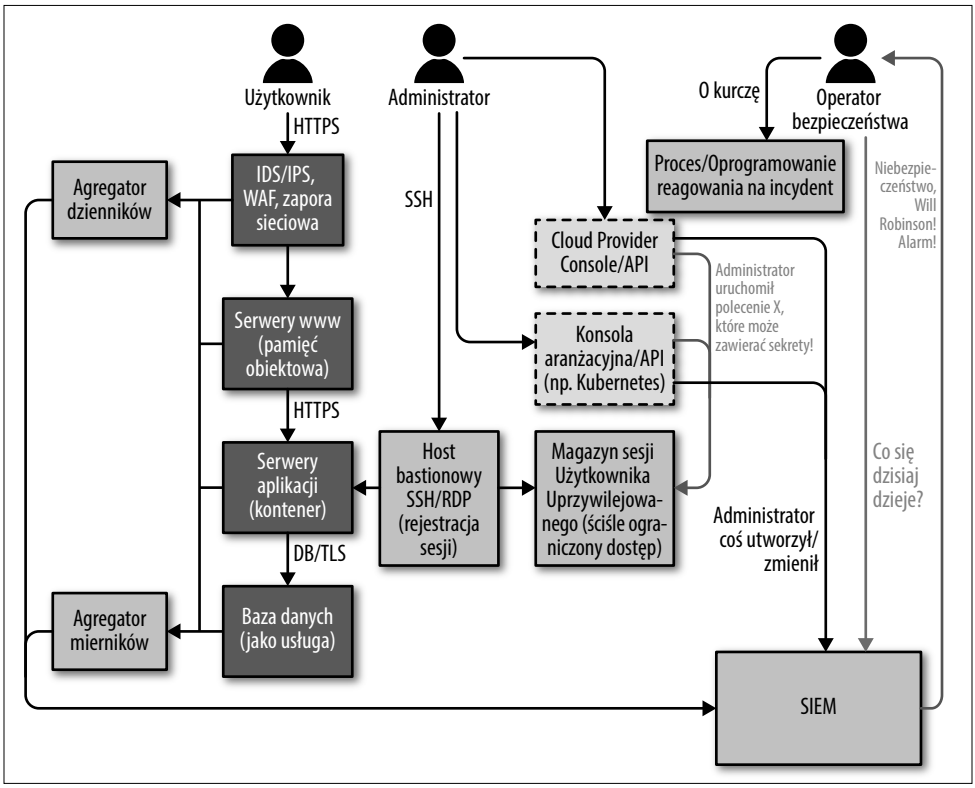
- Amazon GuardDuty może zostać wykorzystany do wyszukiwania nietypowych lub podejrzanych działań na koncie lub w systemach AWS.

- Amazon CloudWatch Logs, Azure Monitor, Google Stackdriver Logging i IBM Cloud Log Analytics umożliwiają przechowywanie i przeszukiwanie dzienników.
- Amazon CloudWatch, Azure Monitor, Google Stackdriver Monitoring i IBM Cloud Monitoring mogą zostać wykorzystane do wyznaczania mierników wydajności.
- AWS CloudTrail, Azure Monitor i IBM Cloud Activity Tracker mogą zostać wykorzystane do monitorowania aktywności użytkowników uprzywilejowanych na kontach w chmurze.
- Azure Security Center może zostać wykorzystany do gromadzenia danych bezpieczeństwa w centralnej lokalizacji, a także do monitorowania integralności plików i innych funkcjonalności bezpieczeństwa.
- Cisco, McAfee i Snort to popularni dostawcy usług wykrywania włamań do sieci, w których ofercie występują urządzenia oparte na środowisku w chmurze.
- CloudFlare, Akamai i Signal Sciences oferują oparte na środowisku w chmurze rozwiązania zapór sieciowych dla aplikacji internetowych.
- OSSEC, Tripwire, AIDE, NT Change Tracker, CloudPassage Halo, Qualys i inne zapewniają tradycyjne lub oparte na środowisku w chmurze rozwiązania do monitorowania integralności plików.
- SIEM, takie jak IBM QRadar, Splunk Security Intelligence Platform, LogRhythm i inni mogą być wykorzystane do zbierania zdarzeń z dzienników, ich analizy oraz do wysyłania powiadomień.
- Wiele popularnych zestawów narzędzi kryminalistycznych, takich jak Encase i FTK, które mają pewne możliwości przetwarzania w środowisku w chmurze.

Połączenie wszystkiego w przykładowej aplikacji

Poniżej przeanalizowano jeszcze raz przykładową aplikację, tym razem z punktu widzenia wykrywania i reagowania. W tym przypadku przyjęty model zagrożenia dotyczy dużej ilości danych o klientach w bazie danych oraz prawdopodobną osobę atakującą, która spróbuje ukraść te dane i sprzedać je w sieci. Należy pamiętać, że postępowanie byłoby nieco inne, gdyby głównym zmartwieniem był przede wszystkim wizerunek naszej marki i zagrożenie polegające na próbie zniszczenia strony internetowej w celu skompromitowania firmy.

Na rysunku 7.2 pokazano wrażliwe systemy rejestrujące zdarzenia związane z bezpieczeństwem oraz sposób, w jaki są obsługiwane przez zespół do spraw bezpieczeństwa. Elementy zaznaczone białym tekstem na ciemnoszarym tle wykorzystywane są do uruchamiania funkcjonalnych części aplikacji. Elementy zaznaczone przerywanymi ramkami oznaczają dostawców chmury lub systemy aranżacji używane do tworzenia infrastruktury aplikacji. Czarnym tekstem na jasnoszarym tle zostały zaznaczone elementy wykorzystywane do uruchamiania struktury audytu. Dla przypomnienia poniżej wymieniono cele aplikacji w zakresie bezpieczeństwa dotyczące wykrywania i reagowania:



Rysunek 7.2. Przykładowa aplikacja z możliwością wykrywania

1. Zbieranie dzienników i mierników, przydatnych zarówno do rozwiązywania problemów operacyjnych, jak i do wykrywania i reagowania na zdarzenia związane z bezpieczeństwem. Wszystkie IDS/IPS, WAF, zapory sieciowe, serwery, bazy danych oraz konsole/interfejsy API są skonfigurowane do rejestrowania istotnych dla bezpieczeństwa zdarzeń i mierników.
2. Przechowywanie dzienników i danych w bezpieczny sposób, tak aby atakujący nie mógł ich usunąć. W praktyce oznacza to szybkie przeniesienie ich z systemu do systemu, który podlega oddzielnej kontroli administracyjnej. W takim przypadku dzienniki są wyświetlane jako przechodzące przez systemy agregujące dzienniki i mierniki, które podlegają oddzielnej kontroli administracyjnej, ale mogą również być wysyłane bezpośrednio do SIEM.
3. Analiza zebranych danych w celu sprawdzenia, czy przedmioty wymagają dalszego badania. W tym przypadku analiza jest przeprowadzana przez połączenie SIEM przy użyciu analizy składniowej dzienników, reguł korelacji, uczenia maszynowego i innych funkcjonalności wymienionych w większości broszur marketingowych SIEM oraz przez mózg operatora do spraw bezpieczeństwa.

4. Automatyczne ostrzeganie o sprawach, które wymagają zbadania przez człowieka. W tym przykładzie SIEM został skonfigurowany do wysyłania powiadomień do osób z rolą operatora bezpieczeństwa. Powiadomienia te mogą być fałszywie pozytywne. Z tego powodu powinna istnieć oddzielna pętla sprzężenia zwrotnego (niepokazana na schemacie), tak aby operatorzy bezpieczeństwa byli w stanie, w miarę możliwości, wykrywać fałszywe alarmy po otrzymaniu fałszywych alarmów, bez maskowania tych prawdziwych.
5. Wykonanie planów reagowania na incydenty oraz odzyskiwania w przypadku podejrzenia faktycznego zdarzenia naruszającego bezpieczeństwo.

Monitorowanie systemów ochronnych

W pierwszym etapie należy zwrócić uwagę na dzienniki utworzone przez systemy ochronne podczas normalnego użytkowania systemu. Na przedstawionym schemacie systemy IDS/IPS, WAF oraz zapory generują dzienniki, powiadomienia i mierniki, gdy system jest używany lub nadużywany. Poniżej przedstawiono kilka przykładów:

- IDS/IPS są wykorzystywane do rejestrowania w sytuacjach, gdy istnieje podejrzenie skanowania portów lub zostanie wykryta znana złośliwa sygnatura.
- WAF jest wykorzystywany do rejestrowania prób ataku typu SQL injection lub deserializacji.
- Zapora sieciowa lub składnik IaaS wykonujący zadania zapory sieciowej są wykorzystywane do rutynowego rejestrowania zaakceptowanych/odrzuconych połączeń, a także do śledzenia mierników ilości ruchu danych wchodzących/wychodzących z sieci na minutę.

Monitorowanie aplikacji

Kolejnym krokiem jest zwrócenie uwagi na dzienniki, które są tworzone przez analizowaną aplikację i infrastrukturę podczas normalnego użytkowania systemu. Dzienniki takie są w dużym stopniu zależne od tego, co wykonuje aplikacja i z jakich komponentów jest złożona. W celach ilustracyjnych założono wykorzystanie wielu różnych technologii i może to być, choć nie musi, projekt dobrej, prawdziwej aplikacji. Poniżej przedstawiono kilka przykładów:

- Serwery www są wykorzystywane do rejestracji każdego żądania, w tym źródłowego adresu IP i żądanego adresu URL. W takim przypadku serwery www to po prostu instancje pamięci obiektowej, które przedstawiają obiekty w odpowiedzi na żądania sieciowe. Usługa przechowywania obiektów jest konfigurowana tak, aby jej dzienniki dostępu, także podczas modyfikowania obiektu, były przesyłane do usługi agregacji dzienników, a mierniki dotyczące liczby żądań były przesyłane do usługi mierników. Dzięki usłudze przechowywania obiektów nie trzeba się martwić o elementy niższego poziomu, takie jak dzienniki systemu operacyjnego, ponieważ te zadania są wykonywane przez dostawcę chmury.

- W analizowanym przykładzie serwery aplikacji są zasobnikami hostowanymi w klastrze Kubernetes. W aplikacji działającej w zasobnikach rejestrowane są wszystkie żądania do standardowego wyjścia (stdout) lub pliku standardowych błędów (stderr) z adresem URL wywoływanego komponentu i odpowiedzią. W takim przypadku aplikacja umożliwia również przesyłanie plików, więc jednym ze składników aplikacji jest klient antywirusowy, który jest wykorzystywany do skanowania każdego przesyłanego pliku i, jeśli zawiera złośliwe oprogramowanie, do poddawania go kwarantannie i wysyłania powiadomienia. Agent rejestrujący w węźle roboczym jest wykorzystywany do wysyłania informacji dziennika z każdego zasobnika, a także z samego węzła roboczego, do agregatora dzienników. Dodatkowo umożliwione jest rejestrowanie kontroli na samym serwerze głównym Kubernetes w celu informowania, kiedy ktoś się do niego uwierzytelni lub utworzy zasobnik.
- Baza danych jest wykorzystywana jako usługa, gdzie rejestrowane są wszelkie próby odmowy dostępu do bazy danych lub określonych tabel w bazie danych, a także wszelkie zmiany w ustawieniach dostępu do bazy danych. Rejestrowane są także mierniki dotyczące ilości danych wysyłanych w danym momencie. Ze względu na to, że kradzież danych z bazy danych jest najpoważniejszym zagrożeniem, naprawdę konieczne jest zwrócenie uwagi na te elementy!
- Infrastruktura wirtualnej chmury prywatnej (niepokazana na rysunku 7.2) jest skonfigurowana do wysyłania mierników sieciowych do agregatora mierników, który z kolei może być wykorzystywany do wysyłania powiadomień do SIEM, w momencie intensywnego użycia sieci.

Monitorowanie administratorów

Konieczne jest również monitorowanie administratorów podczas pracy. Jak wspomniano wcześniej, niekoniecznie jest to równoznaczne z brakiem zaufania wobec administratorów systemu! Oznacza to jedynie przyjęcie założenia, że osoba atakująca jest w stanie uzyskać ważne, administracyjne dane uwierzytelniające za pomocą nikczemnych środków i konieczne jest wykrycie ataku oraz zareagowanie na niego.

W celach edukacyjnych przyjęto następujące założenia:

- Administratorzy są odpowiedzialni za kombinację maszyn wirtualnych i kontenerów w środowisku.
- Administratorzy są w stanie używać, gdy jest to możliwe, chmury oraz funkcjonalności aranżacji kontenerów do uruchamiania określonych poleceń na maszynach wirtualnych i w kontenerach. W sytuacjach awaryjnych administratorzy mogą potrzebować interaktywnej sesji bezpośrednio w systemie.

Na schemacie z rysunku 7.2 dzienniki pełne, które mogą zawierać sekretne informacje, oraz normalne odkażone dzienniki są przechowywane w osobnych systemach, dzięki czemu można ograniczyć dostęp do dzienników pełnych jak najmniejszej liczbie

administratorów. Jeśli oba typy dzienników są przechowywane w tym samym systemie, należy upewnić się, że wszyscy administratorzy tego systemu są upoważnieni do przeglądania pełnych dzienników i że dostęp do nich jest starannie kontrolowany.

Zrozumienie infrastruktury audytu

W tej części została omówiona infrastruktura audytu. W przykładowej aplikacji agregator dziennika, agregator mierników i SIEM zostały pokazane jako osobne systemy, aczkolwiek wiele produktów i usług nakłada się w niektórych, a nawet we wszystkich tych obszarach.

Dodatkowo można mieć produkty lub usługi wysyłające powiadomienia do SIEM lub bezpośrednio do personelu ochrony. Na przykład można wykorzystać systemy analizy ruchu sieciowego do obserwacji nietypowych schematów ruchu sieciowego lub agentów wykrywających punkty końcowe i reagujących, zbierających informacje o aktywności serwerów i stacji roboczych.

Poniżej przedstawiono bardziej szczegółowy opis takich systemów:

- Agregator dziennika może być usługą w chmurze (taką jak Amazon CloudWatch Logs, Azure Monitor, Google Stackdriver Logging, IBM Cloud Log Analytics lub Splunk Cloud) lub oddzielnie zainstalowanym produktem, takim jak Splunk lub Logstash.

  Agregator dziennika powinien znajdować się pod oddzielną od monitorowanych systemów kontrolą administracyjną, tak aby osoba atakująca z dostępem do jednego z monitorowanych systemów nie mogła uzyskać dostępu do agregatora i usunąć dzienników przy użyciu tych samych danych uwierzytelniających. Zalecane jest umieszczenie komponentów kontroli i rejestrowania na osobnym koncie kontrolnym w chmurze, w celu zwiększenia separacji.

  Dzienniki mogą zawierać zarówno informacje niezwiązane z bezpieczeństwem, jak i informacje istotne z punktu widzenia bezpieczeństwa, ale ogólnie tylko dzienniki związane z bezpieczeństwem powinny być przesyłane do SIEM.

- Agregator mierników jest gromadzony przez system mierników, taki jak Amazon CloudWatch, Azure Monitor, Google Stackdriver Monitoring lub IBM Cloud Monitoring, lub przez osobno zainstalowane narzędzie.

- Zarówno system rejestrowania, jak i monitorowania mogą stanowić źródło informacji związanych z bezpieczeństwem dla SIEM. Na przykład system rejestrowania może przesyłać informacje o wszystkich zdarzeniach uwierzytelniania. Natomiast system monitorowania może wywoływać zdarzenie za każdym razem, gdy miernik, jak na przykład szybkość przesyłania, przekroczą określony próg przez określony czas.

- SIEM jest wyposażony w parsery do analizowania różnych typów dzienników oraz w zasady, na podstawie których podejmowana jest decyzja, kiedy warto powiadomić operatora. W takim przypadku reguły SIEM mogą być pomocne w ostrzeganiu,

gdy wystąpią problemy z zalogowaniem się wielu kont w krótkich odstępach czasu (password spraying), gdy zarówno baza danych, jak i mierniki sieciowe wykazują nietypową aktywność lub gdy dzieje się wiele innych kombinacji podejrzanych lub alarmujących zdarzeń.

Podsumowanie

Nawet po zapewnieniu odpowiednich zabezpieczeń, bezpieczeństwo nie jest kompletne, dopóki nie można mieć pewności wykrycia ataku, szybkiej reakcji oraz skutecznego odzyskania.

Wykrywanie dotyczy nie tylko rejestrowania. Nie można po prostu użyć każdego dostępnego źródła tworzenia dzienników i mieć nadzieję, że będzie to przydatne dla bezpieczeństwa. W zależności od użytkowanego środowiska i modelu zagrożeń, konieczne jest określenie, które elementy powinny być obserwowane. Praktycznie we wszystkich środowiskach występują użytkownicy uprzywilejowani, których aktywność należy zawsze obserwować. Należy zadać sobie pytanie: „Jeśli wydarzy się jakaś prawdopodobna zła rzecz, czy będę ją w stanie zaobserwować?". Jeśli nie, konieczne jest zebranie dodatkowych informacji lub upewnienie się, że informacje, które są już zbierane, trafiają we właściwe miejsce i są widoczne.

Po ustaleniu, które komponenty są warte monitorowania, należy upewnić się, że dzienniki i mierniki dla tych komponentów są skutecznie gromadzone i analizowane. W większych środowiskach często konieczne i pomocne jest wykorzystanie SIEM do analizy dużej ilości danych. Istotne jest zapewnienie synchronizacji czasu w różnych systemach oraz przeprowadzenie symulacji ataku tak, aby upewnić się, że rzeczywisty atak nie zostanie przeoczony.

W końcu należy być przygotowanym na poradzenie sobie z udanym atakiem, gdy on nastąpi. Oznacza to zebranie zespołu, niektórych planów i narzędzi przed czasem. W momencie ataku zespół musi rozumieć, jak często przebiegają ataki, jak zablokować środowisko i je wyczyścić oraz, gdy nadszedł czas, jak wezwać dodatkową pomoc.

Podczas wykonywania operacji odzyskiwania, próby oczyszczenia systemu są bardzo ryzykowne. W przypadku gdy ktoś ma dostęp administracyjny, nigdy tak naprawdę nie można być pewnym, że wszystko zostało usunięte, ponieważ istnieje zbyt wiele miejsc, w których można ukryć złośliwe oprogramowanie. Jak dotąd najbezpieczniejszym rozwiązaniem jest usunięcie i następnie przywrócenie każdego zainfekowanego systemu lub też wyrzucenie go i zdobycie nowego. Na szczęście w środowisku w chmurze jest to łatwe do wykonania! Nie należy niedoszacowywać ryzyka wynikającego z próby oczyszczenia na miejscu. Pojedyncze pozwolenie na kontrolę dostępu, pojedynczy wpis w rejestrze w systemie Windows lub inny trudny do znalezienia backdoor może umożliwić osobie atakującej łatwe, ponowne przejęcie systemu.