SYSTEMY MONITOROWANIA I KONTROLI

WSTĘP.

Systemy monitorowania i kontroli (M&C) zapewniają krytyczne usługi dla operacji obliczeniowych poprzez zapobieganie, wykrywanie i reagowanie. Po dostosowaniu do polityki bezpieczeństwa i odpowiednim wdrożeniu systemy te umożliwiają organizacjom wykrywanie incydentów związanych z bezpieczeństwem, ograniczanie ryzyka i analizowanie trendów. Systemy M&C mogą zapobiegać uporczywym próbom nieautoryzowanego logowania z lokalizacji zdalnej, wykrywać problemy z wydajnością sieci pamięci masowej lub ostrzegać osoby reagujące na incydenty o próbie kradzieży własności intelektualnej. Automatyzacja jest kluczowym czynnikiem proaktywnych, skalowalnych wdrożeń systemów M&C w czasie rzeczywistym. Chociaż możliwe jest przeglądanie pojedynczych plików dziennika w ograniczonym zakresie, ręczne przeglądanie dziennika pozostaje niepraktyczne i nieefektywne dla nowoczesnych przedsiębiorstw przetwarzających miliony zdarzeń w sposób rutynowy. Chociaż zakres systemów M&C może różnić się rozmiarem i złożonością, główne komponenty pozostają takie same: gromadzenie danych, redukcja danych i reakcja systemu. Gromadzenie danych obejmuje generowanie i przechowywanie plików dziennika. Systemy komputerowe używają plików dziennika do przechowywania zapisów zdarzeń. Zarejestrowane informacje obejmują czas systemowy, odpowiednie konta użytkowników, identyfikatory systemowe i wykonane działania. Programy zapisują lub dołączają dane do plików dziennika, które są często przechowywane w lokalnych strukturach katalogów i przekazywane do centralnych kolektorów dzienników w celu agregacji. Redukcja danych to proces korzystania z predefiniowanych lub na żądanie reguł i logiki w celu generowania odpowiednich, filtrowanych i możliwych do wykonania widoków zagregowanych danych dziennika. Raporty o wyjątkach, takie jak nieudane lub nieautoryzowane próby logowania, odfiltrowują dopuszczalne zdarzenia, umożliwiając analitykom i automatycznym procesom ostrzegania skupienie się na anomaliach w celu podjęcia dodatkowych działań następczych. Wizualne pulpity nawigacyjne, w tym metryki wydajności i zdarzenia z oceną ryzyka, zapewniają menedżerom informacji i operatorom produkcji korporacyjny wgląd w bieżące działania produkcyjne, które mogą mieć wpływ na cele świadczenia usług. Reakcja systemu obejmuje działania wynikające z fazy redukcji danych. Działania obejmują powiadomienia o alertach, działania naprawcze i procedury odzyskiwania. W zależności od kilku czynników reakcja może być zautomatyzowana lub obejmować informację zwrotną za pośrednictwem interfejsu człowiek-maszyna (HMI). Poniższy kwestionariusz samooceny oparty jest na obszarach omówionych w tym rozdziale; identyfikuje elementy do przeglądu dla istniejącego lub planowanego systemu M&C:

* Jaki jest cel i cel systemu M&C z perspektywy biznesowej i technicznej?

* Jakie są wymagania dotyczące bezpieczeństwa, zgodności, biznesu i prawa?

* Jakie systemy, komponenty lub procesy wymagają monitorowania lub kontroli?

* Jaki model będzie używany do monitorowania lub sterowania celem?

* Gdzie będą przechowywane dane?

* W jaki sposób zapisy danych będą przechowywane i zabezpieczane?

* Jaki rodzaj redukcji danych i raportowania jest wymagany?

* Kto lub co zareaguje na wykryte zdarzenia i incydenty?

* Jakie mechanizmy samoobrony istnieją w systemie M&C?

Zapobieganie, wykrywanie i reagowanie.

Możliwości systemu M&C ogólnie obejmują możliwość zapobiegania, wykrywania i reagowania na wiele zdarzeń. Jednak nie wszystkim wydarzeniom i wyzwaniom trzeba sprostać kosztownymi systemami sterowania lub dedykowanymi czujnikami. Niektóre czynności mogą bardziej nadawać się do monitorowania niż do kontroli. Możesz także chcieć ostrzegać o działaniach, które mogą nie być alarmujące indywidualnie, ale mogą być znaczące łącznie lub przy określonych progach. Decyzje o wdrożeniu i konfiguracji systemów monitorowania i kontroli powinny opierać się na podejściu opartym na ryzyku. Zapobieganie odnosi się do zdolności systemu do zakazania niepożądanego działania. Typowe narzędzia stosowane w bezpieczeństwie sieci obejmują wbudowane systemy zapobiegania włamaniom (IPS) oraz urządzenia do ujednoliconego zarządzania zagrożeniami (UTM). Wdrażanie tych systemów w wąskich punktach, między enklawami i na obrzeżach sieci może ograniczać rozprzestrzenianie się złośliwego oprogramowania w sieci przedsiębiorstwa, a także blokować kanały dowodzenia i kontroli (C&C lub C2) dla klientów botnetów. W dziedzinie bezpieczeństwa fizycznego pułapki jednoosobowe uniemożliwiają jednostkom dostanie się do bezpiecznych obiektów. Wykrywanie odnosi się do zdolności do identyfikowania ataków i innych problemów związanych z bezpieczeństwem za pomocą danych sensorycznych. Systemy opierają się na zautomatyzowanych mechanizmach wykrywania i obserwacji człowieka. Systemy M&C muszą mieć niezawodne mechanizmy wykrywania, aby zarządzać zdarzeniami związanymi z bezpieczeństwem i dostarczać miarodajnych wskaźników dotyczących stanu infrastruktury informatycznej. Proaktywne wykrywanie może obejmować autoryzowane użycie skanera podatności przez testerów kontroli bezpieczeństwa. Wykrywanie reaktywne może obejmować identyfikację źródłowych adresów IP i użytkowników VPN, którzy uczestniczyli w rozproszonej odmowie usługi (DDoS) na sieć dostępną w Internecie. Odpowiedź odnosi się do danych wyjściowych systemów M&C. System monitorowania może wykrywać zdalne próby włączenia FTP i Telnetu na serwerach produkcyjnych, rejestrować aktywność i wysyłać alert administracyjny do operatora lub scentralizowanego mechanizmu korelacji. Jednak system kontrolny korygowałby pliki konfiguracyjne i stany usług lub w ogóle uniemożliwiał wprowadzanie zmian. Po wyświetleniu alertu administracyjnego lub odświeżeniu pulpitu nawigacyjnego może wystąpić dodatkowa reakcja człowieka, na przykład eskalacja do zespołu reagowania na incydenty w celu rozwiązania problemu i analizy pośmiertnej. Brak wykrycia i zgłoszenia naruszeń bezpieczeństwa w określonych ramach czasowych może mieć konsekwencje prawne, ponieważ wiele stanów wymaga powiadamiania o naruszeniu. Wdrażanie głębokiej obrony (zabezpieczenia warstwowe) zwiększa prawdopodobieństwo wykrycia zagrożeń, zapobiegania incydentom i reagowania. Na przykład utrata zasilania prądem zmiennym w zabezpieczonym obiekcie i niereagujący akumulator lub generator rezerwowy mogą uniemożliwić systemowi telewizji przemysłowej (CCTV) zarejestrowanie ataku fizycznego. Dodatkowa warstwa, taka jak ochrona fizyczna, może zapewnić obniżony poziom monitorowania, podczas gdy technicy przywracają zasilanie i systemy monitorowania do normalnej funkcjonalności.

Kontrolowanie kontra monitorowanie.

Monitorowanie odnosi się do obserwacji, rejestrowania i raportowania systemów, komponentów i zdarzeń. Dane zebrane z systemów monitorowania mogą identyfikować intruzów, lokalizować słabe punkty systemu, potwierdzać stan operacyjny i zapewniać potwierdzenie, że kontrole działają online i są na miejscu. W środowisku sieciowym skaner luk w zabezpieczeniach może przeprowadzać uwierzytelnione skanowanie określonych urządzeń w celu zidentyfikowania brakujących poprawek i problemów z konfiguracją bez konieczności modyfikowania lub kontrolowania celów. Systemy M&C działają w dwóch trybach, ciągłym i wsadowym.

1. Tryb ciągły zapewnia ciągły pomiar i zapewnienie zgodności. Systemy, które działają w trybie ciągłym w czasie rzeczywistym, przedstawiają dokładniejszy, co do sekundy wgląd w środowisko operacyjne organizacji.

2. Tryb wsadowy odbywa się w określonych punktach w czasie. Coroczny audyt często wykorzystuje analizę w trybie wsadowym w celu określenia skuteczności kontroli i procesów systemowych. Wyniki dają ograniczoną pewność dla określonego punktu w czasie lub zakresu historycznego w oparciu o dostępne dane.

Kontrola odnosi się do tego, czym możemy manipulować i kontrolować. Zamiast jedynie obserwować i rejestrować informacje o nieautoryzowanych zmianach w środowisku operacyjnym, kontrole mogą ograniczać takie działania w oparciu o predefiniowane konfiguracje i procesy. Kontrole mogą mieć charakter zaporowy lub korygujący w działaniu.

* Zaporowe kontrole zapobiegają wystąpieniu zmiany.

* Kontrole naprawcze przywracają lub przywracają cel kontroli do zatwierdzonego stanu. System zapobiegania włamaniom do hosta (HIPS) może zapobiegać modyfikacjom krytycznych plików systemowych, jednocześnie rejestrując i ostrzegając o nieudanych próbach.

Systemy kontroli zapewniają, że środowisko operacyjne odzwierciedla określone zasady i standardy. Cele kontroli dla technologii informacyjnej i pokrewnej (COBIT) sekcja AI1.9 i ISO 17799 sekcja 9.7 identyfikują potrzebę monitorowania dostępu do systemu i korzystania z niego. Organizacje, które nadal polegają na hasłach do uwierzytelniania, powinny nie tylko ustanowić zasady i projekty procedur w celu spełnienia tych wymagań, ale także wdrożyć techniczne środki kontroli w celu wyegzekwowania zgodności. Jeśli norma przewiduje minimalną długość hasła wynoszącą 15 znaków, z określonymi wymaganiami dotyczącymi złożoności i wymaganym limitem okresu ważności, techniczne kontrole haseł powinny uniemożliwić użytkownikom i administratorom zdefiniowanie niewygasających, krótkich, trywialnych haseł, takich jak abcde. Audytorzy przeprowadzają inspekcję środowiska operacyjnego w celu uzyskania obiektywnej pewności co do środowiska kontroli organizacji. Zazwyczaj audytorzy oceniają próbkę zestawów kontrolnych w zaplanowanych odstępach czasu. Te wykonywane ręcznie czynności w określonym momencie zapewniają wgląd w stopień zgodności infrastruktury. Jednak nie zapewniają one takiego samego poziomu wydajności, jak integracja automatyzacji z ramami, które wspierają ciągłe zapewnianie informacji. Środowisko bezpośrednio wpływa na bezpieczeństwo systemu. Temperatura, wilgotność, jakość powietrza i inne zmienne mogą powodować nieplanowane awarie systemu w środowisku pracy. Takie zmienne, które mogą być poza naszą bezpośrednią kontrolą, również wymagają monitorowania. Aplikacje do zarządzania systemami komputerowymi monitorują wewnętrzne komponenty, a także temperaturę otoczenia i sprzętu oraz poziomy napięcia zasilania. Większość organizacji może nie być w stanie kontrolować temperatury przegrzewającego się procesora lub braku energii elektrycznej dostarczanej przez zakład energetyczny, ale progi sensoryczne w aplikacji monitorującej mogą uruchamiać automatyczne skrypty lub powiadamiać lokalny personel o zainicjowaniu zamknięcia systemu. W takich sytuacjach progi monitorowania i alerty zapewniają systemom i operatorom możliwość łagodnego zatrzymania uruchomionych procesów lub przywrócenia przetwarzania do alternatywnego systemu lub lokalizacji. Organizacje decydują się na wdrożenie systemów z możliwościami monitorowania lub kontroli z wielu powodów, w tym postrzeganego ryzyka, kosztów finansowych, trudności logistycznych i wartości biznesowej. W przypadku organizacji z niedojrzałym programem bezpieczeństwa i ograniczonym wglądem w środowisko operacyjne monitorowanie może również zapewnić sposób przejścia do przyszłych kontroli. Na przykład monitorowanie może dostarczać danych bazowych i umożliwiać raportowanie wykorzystania zasobów organizacji (np. miejsca na dysku, korzystania z Internetu) oraz

stanowić podstawę do efektywnego planowania („Między sierpniem a listopadem przyszłego roku zabraknie nam miejsca na dysku") a także wskazuje obszary, w których należy zwiększyć świadomość, szkolenia, edukację i przestrzeganie przepisów („Czterech naszych pracowników jest łącznie odpowiedzialnych za 60 procent wykorzystania przepustowości łącza internetowego — a połowa ich działalności polega na oglądaniu filmów pornograficznych w godzinach pracy!").

Pętla kontrolna.

W większości środowisk ludzie pozostają w pętli kontrolnej. Pętla sterowania składa się ze sterownika, systemu docelowego, toru komunikacji dwukierunkowej oraz przesyłanych danych. Pętla kontrolna jest uważana za pętlę zamkniętą, gdy proces jest zautomatyzowany i nie wymaga interakcji człowieka; otwarta pętla obejmuje interakcję człowieka. Wymagania systemu określają typ pętli. Gdy czujniki rurociągu gazowego wykryją nagły spadek ciśnienia, zautomatyzowany system sterowania może wymagać natychmiastowego zablokowania w celu wyizolowania wycieku i wysłania powiadomień ostrzegawczych. Pozostawienie otwartego obiegu i oczekiwanie na reakcję człowieka może skutkować niepożądanymi stratami produktu oraz wyzwaniami środowiskowymi i prawnymi. W przypadku wdrażania poprawek systemu operacyjnego otwarta pętla umożliwiłaby systemowi przesłuchiwanie hostów, określanie poziomów poprawek i raportowanie stanu w celu dalszej analizy i podjęcia działań. Następnie przełożony może zatwierdzić określone poprawki do poszczególnych systemów po przeprowadzeniu wystarczających testów na niekrytycznych, nieprodukcyjnych systemach i koordynacji z interesariuszami systemu. Chociaż w pełni zautomatyzowane instalowanie poprawek oprogramowania może wydawać się wykonalnym procesem, wiąże się ono z dodatkowym ryzykiem (poprzez zakłócenia w systemie i procesach) oraz problemami ze zgodnością. W przypadku automatyki przemysłowej i sterowania określone aktualizacje mogą nie być certyfikowane do użytku i wymagać kontaktu ze sprzedawcą lub weryfikacji na stronie pomocy technicznej.

Definiowanie zakresu i wymagań systemowych.

Aby systemy M&C działały efektywnie, kierownictwo musi jasno określić zakres i wymagania systemowe. Zakres w szczególności odnosi się do odpowiednich procesów i osób wchodzących w interakcję ze środowiskiem komputerowym. Na przykład, aby monitorować dział badań i rozwoju (R&D) pod kątem komunikacji sieciowej dotyczącej własności intelektualnej, zakres może obejmować personel pomocniczy IT/IS, współdzielone zasoby sieciowe i istniejące procesy komunikacji ze zdalnymi lokalizacjami i działami zewnętrznymi. Wymagania systemowe odnoszą się do możliwości niezbędnych do wykonywania pożądanych funkcji M&C. Pracując nad wymaganiami, należy pamiętać, że mechanizmy zapobiegania i kontrole w rzeczywistych środowiskach mogą ostatecznie zawieść lub stać się przestarzałe z powodu zmian technologicznych. Wymagania dotyczące monitorowania prac badawczo-rozwojowych mogą obejmować potrzebę przechwytywania pakietów w czasie rzeczywistym, algorytm identyfikacji własności intelektualnej, automatyczne alerty i odpowiednio zabezpieczone urządzenie zbierające.

Zainstalowanie portu testowego dostępu do sieci (TAP) na łączu sieciowym, a następnie zapisanie przechwyconego ruchu do kolektora danych w celu przyszłej analizy może wydawać się logiczne. Jeśli jednak badanie witryny wykryje użycie nieudokumentowanych modemów komórkowych, niezaszyfrowanych bezprzewodowych hotspotów i osobistych kont e-mail do poufnej komunikacji, sieć TAP nie spełni pierwotnego celu. W tym przypadku wymagania M&C rozszerzają się o ograniczniki sygnału (klatka Faradaya), obowiązkowe ograniczenia urządzeń, kontrolę dostępu do sieci (NAC), wymuszone zasady komunikacji IPSec i filtry sieciowe. Okresowe szkolenia w zakresie świadomości bezpieczeństwa i odświeżanie polityki mogą być również konieczne, aby zapewnić, że organizacja jasno komunikuje oczekiwania dotyczące korzystania z osobistej poczty elektronicznej i innych środków

komunikacji elektronicznej oraz urządzeń. Musimy również wziąć pod uwagę możliwości systemu M&C, w tym niezamierzone konsekwencje zbędnych funkcji i możliwości wdrożonego systemu. Na przykład system oparty na komputerze PC używany do zarządzania fizycznym systemem plakietek bezpieczeństwa może być również używany przez operatora do podłączania urządzeń USB, grania w gry wideo i łączenia się z Internetem w celu udostępniania plików peer-to-peer (P2P). Problemy te można częściowo złagodzić poprzez wzmocnienie zabezpieczeń systemu, narzędzia oparte na agentach i projektowanie sieci. Panele dystrybucyjne podłączone do czytników kart wykonują bardziej specyficzne, restrykcyjne funkcje przetwarzania niż komputer PC lub serwer towarowy; w przypadku paneli uwaga byłaby skierowana na fizyczny dostęp do urządzeń i toru komunikacji. Wymagania dotyczące zgodności i program bezpieczeństwa organizacji mają wpływ na wdrożenie systemów M&C. Przepisy mogą wymagać kontroli dostępu w celu ograniczenia informacji do upoważnionych użytkowników oraz wystarczającego monitorowania w celu wykrycia nieautoryzowanych prób uzyskania dostępu do zasobów informacyjnych. W odpowiedzi na ustawę HIPAA organizacja może być zmuszona do zintegrowania dodatkowych procedur przeglądu dzienników, a także odpowiednich środków kontroli wszystkich systemów i procesów, które dotykają lub potencjalnie przekazują dane osobowe (PII). Spółka publiczna potrzebuje odpowiednich kontroli, aby zapewnić dokładną sprawozdawczość finansową. Polityka bezpieczeństwa może odwoływać się do konieczności przestrzegania przepisów Sarbanes-Oxley Sekcja 404. Zakres systemu M&C musiałby wówczas obejmować zasoby obliczeniowe, przepływy procesów informacyjnych oraz personel mający dostęp do systemu informacji finansowych. Systemy M&C powinny odzwierciedlać oczekiwania polityki bezpieczeństwa organizacji i pasować do odpowiednich ram, takich jak COBIT. Wykorzystanie struktury kontroli zapewnia logiczne zarządzanie systemami M&C. Ramy umożliwiają kierownictwu dalsze zrozumienie procesów przedsiębiorstwa i określenie potrzeby ograniczenia lub akceptacji ryzyka. PO9.7 w COBIT identyfikuje systemy kontroli jako część części zarządzania ryzykiem związanej z wyborem zabezpieczeń.

MODELE SYSTEMU

Wewnętrzne, jeden-do-jednego, jeden-do-wielu i rozproszone.

Systemy M&C można podzielić na cztery ogólne modele: wewnętrzny, jeden-do-jednego, jeden-do-wielu i rozproszony. Rodzaj zastosowanego modelu zależy od złożoności systemu i rodzaju wymaganych informacji. Modele te mogą obejmować systemy autonomiczne, jak również te, które wymagają interakcji człowieka.

1. System wewnętrzny jest jedną z najprostszych form M&C; monitoruje lub kontroluje się. Pojedynczy serwer lub urządzenie sieciowe może monitorować wykorzystanie procesora lub inne komponenty systemu w celu oceny problemów z wydajnością systemu. Z punktu widzenia kontroli system wewnętrzny może zabraniać określonych działań, takich jak nieautoryzowane próby modyfikacji plików systemowych lub lokalnego logowania do systemu.

2. Model jeden do jednego umożliwia jednemu systemowi monitorowanie lub sterowanie innym niezależnym systemem. W przypadku skalowania w dużym środowisku model ten może stać się uciążliwy i skutkować niepotrzebnym powielaniem usług i przetwarzania IT. Na przykład program do planowania zadań przedsiębiorstwa monitorujący pojedynczy serwer aplikacji finansowych może określić, kiedy pliki są dostępne do przetworzenia. Jeśli inne systemy w tym samym środowisku obsługują niezależne programy do planowania zadań, operatorzy będą potrzebować dodatkowego czasu na monitorowanie i rozwiązywanie problemów z powielonymi funkcjami. Jednak model jeden do jednego może być całkiem przydatny w określonych sytuacjach o wysokiej dostępności, które wymagają przełączania awaryjnego. Zapora sieciowa lub serwer o znaczeniu krytycznym stale

monitoruje i odzwierciedla konfigurację oraz informacje o sesji systemu podstawowego. W przypadku awarii systemu podstawowego system monitorowania przejmie funkcje produkcyjne, aby uniknąć znacznych zakłóceń w środowisku biznesowym.

3. Model jeden do wielu jest najczęściej spotykany w środowiskach korporacyjnych. Centralny system monitorowania i sterowania zdalnie zarządza wieloma systemami. Z centralnego punktu wszystkie cele mogą być przesłuchiwane i aktualizowane bez potrzeby ręcznych zmian jeden do jednego. Scentralizowana M&C może również obniżyć koszty, upraszczając funkcje M&C wielu zasobów w różnych lokalizacjach. Model ten poprawia również efektywność audytu, ponieważ w celu sprawdzenia kontroli i zmian w środowisku należy przejrzeć mniej źródeł informacji.

4. Model rozproszony obejmuje czujniki i elementy sterujące rozproszone w całym środowisku. Elementy sterujące mogą działać niezależnie lub zdalnie z wejściem z centralnego systemu sterowania. Węzły mogą służyć jako lokalny serwer proxy lub przekazywać informacje bezpośrednio do centralnego kolektora w celu bezpiecznego zarządzania dziennikami, raportowania i redukcji danych. W przypadku organizacji, które próbują zarządzać urządzeniami heterogenicznymi, model rozproszony umożliwia personelowi wdrażanie najlepszych komponentów M&C dla określonych systemów, przy jednoczesnym zachowaniu możliwości agregowania danych w scentralizowanym repozytorium. Ten poziom agregacji zapewnia szerszy wgląd w zmiany w infrastrukturze.

Automatyzacja i interfejs człowiek-maszyna .

Automatyzacja umożliwia systemom M&C zbieranie informacji sensorycznych i inicjowanie reakcji bez konieczności interakcji człowieka. Wiele systemów informatycznych działa przez całą dobę i generuje duże ilości dzienników zdarzeń. Delegowanie personelowi operacyjnemu zadania polegającego na ręcznym przeglądaniu milionów wpisów dziennika i korelowaniu ich w celu uzyskania istotnych informacji jest niepraktyczne. Celem systemów M&C jest uzyskanie znaczących informacji z systemów docelowych oraz zgłaszanie i korygowanie anomalii. Automatyzując gromadzenie i redukowanie danych, menedżerowie i pracownicy mogą przeglądać skonsolidowane podsumowania zdarzeń i reagować na sytuacje, które nie zostały jeszcze automatycznie przefiltrowane lub kontrolowane. Interfejs człowiek-maszyna (HMI) to punkt, w którym operator komunikuje się z systemem monitorowania lub sterowania. W środowiskach przemysłowych oprogramowanie pośredniczące HMI przekształca czynności systemowe w interaktywne ekrany z wystarczającymi możliwościami, aby personel mógł wykonywać określone zadania. Prezentacja danych jest ważnym czynnikiem dla HMI. Operatorzy muszą mieć możliwość wykonywania swoich funkcji zawodowych i zachowania odpowiedniej świadomości sytuacyjnej, bez dostępu do niezbędnych lub rozpraszających uwagę elementów systemu. W typowych sieciowych środowiskach operacyjnych rolę interfejsu HMI pełnią interaktywne interfejsy WWW. Analityk może przeglądać zakodowane alerty sygnalizacji świetlnej (czerwony, żółty, zielony) w interfejsie internetowym i wykonywać kroki dochodzeniowe w celu segregacji i rozwiązywania otwartych problemów. W niektórych sytuacjach organizacje wykorzystujące automatyzację mogą odnieść korzyści z poprawy bezpieczeństwa pracowników i skrócenia czasu reakcji. Autonomiczne pojazdy i urządzenia wciąż się mnożą. Departament Marynarki Wojennej USA wykorzystuje bezzałogowe pojazdy podwodne (UUV)7, które odzwierciedlają model rozproszony, realizując autonomiczne działania, z wymianą informacji poprzez siatkę czujników w ramach Globalnej Sieci Informacyjnej (GIG). Systemy te mogą monitorować zmienne środowiskowe, wykrywać zagrożenia, takie jak niewybuchy, reagować na zmiany i komunikować się z właścicielami systemów. Podobnie jak systemy wykrywania i zapobiegania włamaniom w środowisku sieciowym, UUV mogą wykonywać funkcje, które mogą być nieodpowiednie dla bezpośredniej interakcji człowieka. Oba mogą prowadzić ciągłe monitorowanie i gromadzić duże ilości informacji, których nie można było zebrać ręcznie. Ponadto, podobnie jak systemy zapobiegania włamaniom w środowisku sieciowym, UUV może

wykrywać zagrożenie, ostrzegać pobliskie UUV i zgłaszać stan za pośrednictwem GIG. Rosnące wykorzystanie sztucznej inteligencji (AI) i zasobów robotycznych zapewnia dodatkowe możliwości mobilnej i autonomicznej M&C. Humanoidalny robot przeciwpożarowy SAFFiR z Laboratorium Badawczego Marynarki Wojennej Stanów Zjednoczonych to kolejny przykład reagowania na zagrożenia środowiskowe bez narażania tradycyjnej siły roboczej na niebezpieczne zadania podczas pracy w zespole. Chociaż SAFFiR może nie zastąpić systemu tłumienia gazów w centrum danych, sztuczna inteligencja w centrum danych była widziana w walce z niechcianymi komercyjnymi wiadomościami e-mail i spamem. Podczas wdrażania zautomatyzowanych zasobów, wdrażania sztucznej inteligencji czy zdalnego dowodzenia pojazdami bezzałogowymi integralność systemu i bezpieczeństwo ścieżek komunikacyjnych mają kluczowe znaczenie. Niewłaściwy dostęp fizyczny, przepełnienie bufora oprogramowania, słabe poświadczenia administracyjne i infekcje USB złośliwym oprogramowaniem to powszechne sposoby na naruszenie integralności systemu M&C. W środowiskach sieciowych inżynier sieciowy może używać pozapasmowych ścieżek komunikacyjnych do łączenia się z interfejsem HMI przez port konsoli, aby uniknąć typowych ataków sieciowych na interfejs zarządzania. Używanie niezabezpieczonych metod komunikacji do aktualizacji systemów M&C lub zarządzania nimi przez niezaufane ścieżki to kolejny powszechny sposób narażania M&C na nieautoryzowany dostęp i naruszenie bezpieczeństwa. Migracja z uwierzytelniania FTP, Telnet i hasła do Secure Shell (SSHv2) z uwierzytelnianiem za pomocą pary kluczy to jeden z praktycznych sposobów zmniejszenia części tego ryzyka do bardziej akceptowalnego poziomu. W przypadku sieciowych IPS w odpowiednio przygotowanym środowisku sieciowym można wykrywać anomalie ruchu przypominające robaki, kierować je do tarpitów sieciowych i przekazywać raporty krzyżowe do dodatkowych czujników. W takiej sytuacji zautomatyzowana reakcja jest znacznie szybsza i potencjalnie mniej uciążliwa niż użycie systemu wykrywania włamań (IDS; tylko monitorowanie) z alertami kierowanymi do dyżurnego analityka w celu dalszych działań następczych.

Migawki a czas rzeczywisty.

Migawki zapewniają widok systemu docelowego z punktu w czasie. Audytorzy używają ich do regularnie planowanych audytów. Comiesięczne skanowanie środowiska w celu potwierdzenia zgodności może również ujawnić trendy w zakresie bezpieczeństwa w środowisku. Raporty trendów identyfikują skuteczność zabezpieczeń w czasie. Organizacja może zauważyć gwałtowny spadek podatności na zagrożenia po audycie zewnętrznym. Z biegiem czasu, bez stabilnego programu zarządzania podatnościami, liczba podatności powróci do poziomów sprzed audytu. Migawki nie dostarczają natychmiastowych ani bieżących informacji o zmianach lub działaniach naprawczych wprowadzonych do systemów produkcyjnych. Ponadto migawki nie będą sprawdzać, czy formant działa przez cały czas, tylko w czasie, w którym wykonano migawkę. Używanie miesięcznych migawek do przeglądania systemu, który często się codziennie zmienia, nie zapewni takiego samego poziomu pewności, jak M&C w czasie rzeczywistym. Monitorowanie w czasie rzeczywistym odnosi się do trwałej, ciągłej obserwacji celu. Sterowanie w czasie rzeczywistym odnosi się do zdolności systemu sterowania do aktywnego wpływania na cel. Przemysłowe środowiska zależą od informacji zebranych w czasie rzeczywistym w ramach M&C. Gdy skroplony gaz ziemny (LNG) przepływa przez terminal LNG, operatorzy nie powinni czekać, aż cysterna będzie pusta, aby potwierdzić, że jakikolwiek produkt został pomyślnie przeniesiony do zbiorników magazynowych. System M&C może stale monitorować objętość produktu opuszczającego zbiornik, porównywać te dane z objętością wchodzącą do pojemnika do przechowywania, uruchamiać alarmy w przypadku wykrycia wycieku i inicjować odcięcie, aby uniknąć utraty produktu. Podczas alokacji i dystrybucji zasobów w celu zaspokojenia zapotrzebowania monitorowanie w czasie rzeczywistym zapewnia nadzorcom natychmiastowe zrozumienie obszarów potrzeb. W środowisku sieciowym może to obejmować szczytowe wykorzystanie sieci podczas cyklu rozliczeniowego lub trendy zakupów online spowodowane świętami. Internetowy portal zakupowy,

który wykorzystuje przetwarzanie w chmurze do alokacji zasobów, może wykorzystywać monitorowanie w czasie rzeczywistym do przejrzystego wykrywania i udostępniania lub anulowania aprowizacji zasobów obliczeniowych i pamięci masowej w oparciu o zapotrzebowanie klientów. Witryny internetowe narażone na ataki rozproszonej odmowy usługi (DDoS) mogą korzystać z monitorowania w czasie rzeczywistym w celu zidentyfikowania incydentu i kontroli w czasie rzeczywistym w celu zablokowania lub ograniczenia niepożądanego ruchu. Aby zminimalizować wpływ, można również wykorzystać usługę buforowania sieci Web lub sieć dostarczania treści (CDN). Na obszarach przemysłowych monitorowanie w czasie rzeczywistym może wykrywać, gdzie zarządcy sieci elektroenergetycznych powinni skierować dodatkowe źródła energii, aby zaspokoić popyt, ile pobierać z rezerw, a także kiedy wdrażać kontrole w czasie rzeczywistym, aby wymusić ciągłe przerwy w dostawie prądu i zapewnić integralność sieci. DS13.3 w COBIT 4.1 identyfikuje potrzebę odpowiedniego rejestrowania zdarzeń w celu analizowania działań w czasie. Jednak bez dobrze zaplanowanych zautomatyzowanych procesów i redukcji danych ilość danych generowanych z migawek i działań w czasie rzeczywistym przytłoczy personel. Poprzez scentralizowane gromadzenie i redukowanie danych, wyznaczeni aktorzy mogą oceniać wyniki zarówno raportów w czasie rzeczywistym, jak i migawek. Ta kombinacja może identyfikować ogólne trendy, zapewniać nieprzerwane działanie systemów M&C i zabezpieczać dowody zidentyfikowanego ataku

Zrzuty pamięci.

Zrzuty pamięci to reprezentacje danych w pamięci w określonym momencie. Zrzuty pamięci są najczęściej używane po a awarii systemu, ale są również przydatne w badaniach kryminalistycznych, gdy śledczy chcą uzyskać z systemu maksymalną możliwą ilość informacji. Istnieją dwa podejścia do uzyskiwania kopii pamięci: w trybie online, przy użyciu narzędzi diagnostycznych podczas działania systemu, oraz w trybie offline, z magnetycznych nośników pamięci, na które kopiowane są regiony pamięci.

Narzędzia diagnostyczne.

Narzędzia diagnostyczne to procedury oprogramowania systemowego, których można używać do debugowania. Programy te, znane również jako narzędzia do debugowania, działają z maksymalnymi uprawnieniami (na poziomie administratora, administratora lub ich odpowiedników) i umożliwiają uprzywilejowanemu użytkownikowi przeglądanie lub modyfikowanie dowolnej części pamięci. Narzędzia zwykle drukują lub wyświetlają zawartość obszarów pamięci w różnych formatach, takich jak binarny, ósemkowy (o podstawie 8) lub szesnastkowy (o podstawie 16), z konwersją do ASCII dla łatwiejszej czytelności. Narzędzia zazwyczaj zapewniają natychmiastowy dostęp do struktur pamięci, takich jak bufory terminali, które pozwalają analitykowi zobaczyć, co poszczególni użytkownicy piszą lub widzą na swoich ekranach, bufory plików zawierające dane przesyłane do lub z określonych otwartych plików, bufory (bufory wydruku) oraz regiony specyficzne dla programu, takie jak stosy danych. Ponieważ narzędzia do debugowania umożliwiają również modyfikację regionów pamięci, należy ich używać z najwyższą ostrożnością; ze względów bezpieczeństwa mądrze jest sformułować zasadę, że żadne narzędzie do debugowania z dostępem administratora nie może zostać uruchomione bez obecności dwóch osób. W operacjach o wysokim poziomie bezpieczeństwa dane wyjściowe narzędzi do debugowania powinny być rejestrowane w plikach papierowych, aby udowodnić, że przy użyciu tych programów nie przeprowadzono żadnych nieautoryzowanych operacji. Dostęp do uprzywilejowanych programów do debugowania powinien być ściśle kontrolowany, na przykład za pomocą ścisłych list kontroli dostępu lub nawet szyfrowania przy użyciu zastrzeżonych kluczy.

Wyjście na nośniki magnetyczne lub papier.

Jedną z metod wykonywania zrzutu pamięci i dalszej analizy jest kopiowanie danych z pamięci na nośniki magnetyczne, takie jak taśma, dyski wymienne lub płyty DVD wielokrotnego zapisu. Chociaż kiedyś praktyczne było wydrukowanie całej zawartości pamięci na papierze, gwałtowny wzrost rozmiarów pamięci sprawia, że takie drukowanie jest niepraktyczne w dzisiejszych systemach. Na przykład w 1980 r. duży wieloużytkownikowy minikomputer mógł mieć 1 MB (megabajt) dostępnej pamięci RAM, co skutkowało łatwym do zarządzania stosem papieru o grubości pół cala. W chwili pisania tego tekstu częściej spotyka się systemy biznesowe z 64-bitowymi procesorami i ponad 4 GB (4000 MB) pamięci. Z perspektywy czasu relatywnie starszy komputer z zaledwie 256 MB pamięci wygenerowałby pojedynczy wydruk o grubości kilku stóp. Dlatego kopiowanie pamięci na statyczny nośnik pamięci jest preferowane do przyszłej analizy zrzutów pamięci po awariach systemu, infekcjach nieznanym złośliwym oprogramowaniem i incydentach wymagających interwencji kryminalistycznej.

Poruszanie się po zrzucie za pomocą narzędzi eksploracyjnych.

W systemach produkcyjnych korzystających z niezawodnych systemów operacyjnych awarie są rzadkie i zazwyczaj dokładnie badane w celu zidentyfikowania przyczyn anomalii. Zasadniczo po utworzeniu zrzutu należy go przestudiować, szukając problemu, a następnie go poprawiając. W przypadku systemów o dużej pamięci narzędzia eksploracyjne służą do przyspieszenia wyszukiwania problemów w zrzucie, umożliwiając analitykowi znalezienie dowolnej nazwanej tabeli systemowej lub innego obszaru pamięci. Na poziomie kryminalistycznym haszowanie może być również używane do filtrowania znanych dobrych i znanych złych elementów w archiwum pamięci.

Zrozumienie tabel systemowych.

Tabele systemowe to katalogi danych systemowych, w których każdy punkt odniesienia jest identyfikowany przez przypisaną etykietę, pozycję w tabeli lub wskaźniki z innych tabel. Zrozumienie tabel systemowych jest niezbędne do analizy problemów systemowych. Niezależnie od szczegółów systemu operacyjnego i specyficznych dla systemu nazw tabel, niektóre z ważnych tabel systemowych obejmują:

* Tabela kontroli procesu. Wskaźniki do tabel procesów dla każdego procesu uruchomionego w systemie lub uruchomionego w momencie uzyskania kopii pamięci

* Tabele procesów. Szczegółowe informacje o każdym procesie ze wskaźnikami do wszystkich tabel dla tego konkretnego procesu

* Stosy danych. Wszystkie zmienne używane przez określone procesy

* Bufory. Dane przesyłane do lub z plików i urządzeń, takich jak dyski i terminale

* Tabele zarządzania pamięcią. Listy dostępnych bloków pamięci

* Tabele komunikacji między procesami. Na przykład informacje o blokowaniu zasobów lub wszelkich flagach logicznych używanych przez wiele procesów

Praca z kimś, kto rozumie szczegółową strukturę tabel systemu operacyjnego, może mieć kluczowe znaczenie dla prac związanych z bezpieczeństwem, w których badacze muszą dokładnie określić, co się stało podczas włamania lub innego nieautoryzowanego użycia systemu.

Zagadnienia dotyczące bezpieczeństwa danych zrzutu. Zrzuty pamięci muszą być zabezpieczane podczas używania i niszczone w razie potrzeby. Zrzut zawiera całość informacji o systemie w pamięci, w tym takie dane jak:

* Hasła, które właśnie zostały wpisane do buforów terminala w celu zmiany logowania lub dostępu do zastrzeżonych podsystemów i aplikacji

* Klucze szyfrujące

* Dane poufne pozyskane z akt zastrzeżonych i nieupoważnione do wizualizacji przez personel operacyjny (np. dane medyczne z akt osobowych)

* Dane finansowe, które mogłyby zostać wykorzystane w oszustwach

* Informacje dotyczące bezpieczeństwa narodowego ograniczone do wyższych poziomów dostępu niż administracja systemem

ZARZĄDZANIE LOGAMI

Generowanie dziennika.

Plik dziennika zawiera zapis zdarzeń. Ten rekord jest podstawowym budulcem systemów M&C. Pliki te służą jako cyfrowa ścieżka audytu działań systemowych. Systemy operacyjne, bazy danych i aplikacje mogą zawierać wbudowane funkcje rejestrowania. Jednak rejestrowanie nie zawsze jest włączone lub skonfigurowane do użytku i agregacji. System monitoruje działania i zapisuje odpowiednie informacje jako wpis w pliku dziennika. Pliki dziennika systemu operacyjnego śledzą problemy z aplikacjami, próby dostępu i problemy ogólnosystemowe. Progi i rozmiary plików można dostosować do wymagań środowiska. Może nie być konieczne zapisywanie wpisu w dzienniku za każdym razem, gdy użytkownik pomyślnie otworzy lub zamknie plik w udziale sieciowym hostowanym na woluminie pamięci masowej, ale może być konieczne rejestrowanie i raportowanie prób dostępu uprzywilejowanego do konsoli zarządzania lub połączeń zdalnych przez Bezpieczna powłoka (SSH). Dzienniki transakcji idą o krok dalej, przechowując kopie rzeczywistych zmian wprowadzonych w systemie. Mają stały rozmiar, automatycznie generując nowy plik dla przyszłych transakcji. Najczęściej spotykane w bazach danych dzienniki transakcji mogą służyć do odbudowy uszkodzonej bazy danych. Używając znanej dobrej kopii zapasowej bazy danych i dzienników transakcji z kopii zapasowej bazy danych do chwili obecnej, bazy danych można odtwarzać do niezawodnego punktu w czasie przed awarią. Dzienniki transakcji powinny być aktywnie monitorowane, ponieważ mogą szybko zająć duże ilości pamięci. Zazwyczaj zatwierdzone dzienniki transakcji są czyszczone po pomyślnym utworzeniu kopii zapasowej. Inne typy dzienników, takie jak ruch w witrynie, mogą automatycznie generować nowe pliki dziennika raz dziennie; te dzienniki mogą nie zawierać całych transakcji Witryny, ale identyfikują odwiedzającego na podstawie wcześniej zdefiniowanych kryteriów. Kluczem jest tutaj elastyczność w określaniu, co będzie monitorowane i jaki format będzie najlepszy do generowania dziennika Zasady przechowywania danych muszą jasno określać, jak długo dane powinny być przechowywane, zgodnie z wymaganiami zewnętrznymi i polityką wewnętrzną. Wymagania dotyczące przechowywania mogą wynosić od 1 do 6 lat, podczas gdy niektóre dane mogą wymagać przechowywania na nośnikach kopii zapasowych przez czas nieokreślony ze względu na obowiązek ich przechowywania na mocy przepisów prawa. Archiwizacja i przechowywanie plików dziennika stają się z czasem problematyczne: pliki dziennika na poziomie systemu mogą osiągnąć maksymalny rozmiar i zastąpić istniejące dane dziennika lub spowodować zamknięcie systemu; scentralizowane systemy zarządzania dziennikami mogą spowolnić do indeksowania podczas wysyłania zapytań do relacyjnej bazy danych w celu wyeksportowania danych do pliku płaskiego. Systemy gromadzenia i analizy dzienników muszą być skalowalne, ponieważ częstość i liczba zdarzeń może z czasem rosnąć lub pękać. Niektóre organizacje radzą sobie z tymi rozbieżnościami poprzez włączenie usług rejestrowania i przechowywania w chmurze, podczas gdy inne polegają na bardziej tradycyjnych, wewnętrznych rozwiązaniach pamięci masowej.

Typy rekordów pliku dziennika.

Plik dziennika (znany również jako ścieżka audytu) tradycyjnie zawiera zapisy dotyczące transakcji, które mają zaktualizowane pliki online lub w inny sposób reprezentują interesujące zdarzenia (np. logowanie do systemu lub inicjowanie procesu). Niektóre pliki dziennika bazy danych lub aplikacji mogą również zawierać kopie rekordów, na które miało to wpływ przed zarejestrowaną transakcją lub po niej. Istnieje wiele różnych typów rekordów plików dziennika, a każdy z nich zawiera określony rodzaj informacji. Zazwyczaj wszystkie rekordy dziennika systemu operacyjnego są przechowywane w plikach o maksymalnym skonfigurowanym rozmiarze i są identyfikowane przez monotonicznie rosnące numery plików. Gdy plik się zapełni, system operacyjny otwiera kolejny, którego identyfikatorem jest kolejny numer w sekwencji. Ponieważ rekordy pliku dziennika różnych typów mają różne rozmiary, w niektórych systemach operacyjnych plik dziennika jest definiowany ze zmienną długością rekordu.

Rozruch systemu.

Rekord dziennika rozruchu systemu zawiera informacje dotyczące rozruchu lub uruchamiania komputera. Ponieważ jest to związane z konkretną działalnością i ogólnie do określonego obszaru sprzętu lub nośnika, informacje dotyczące rozruchu mogą okazać się pomocne, gdy rozruch się nie powiedzie i konieczna będzie analiza.

Zamknięcie systemu.

Rekord dziennika zamknięcia systemu zawiera informacje o tym, kiedy system został zamknięty i przez kogo. Informacje te mogą być nieocenione przy próbie analizy problemu lub znalezienia sabotażysty. W systemach, które obejmują wyłączenia awaryjne (np. przez wywołanie procedur, takich jak nagła śmierć, gdy parametry systemu wykroczą poza dopuszczalny zakres), rekord zamknięcia może zawierać określone informacje o przyczynie wyłączenia awaryjnego. Z punktu widzenia bezpieczeństwa, godne zaufania zapisy rozruchu i zamknięcia systemu mogą zapobiec ukryciu przez złoczyńcę zamknięcia, po którym nastąpił nieautoryzowany rozruch podsystemu diagnostycznego, który umożliwiłby manipulację plikami bez zapisów dziennika w celu śledzenia operacji. Rekordy rozruchowe pokazywałyby niewyjaśnioną lukę między wyłączeniem a rozruchem.

Inicjacja procesu.

Proces rozpoczyna się, gdy określony program jest ładowany i uruchamiany przez określonego użytkownika w określonym czasie. Rekordy dziennika inicjowania procesów pokazują, kiedy różne procesy zostały zainicjowane i kto je zainicjował. Pliki te zapewniają metodę śledzenia aktywności pracowników, a także monitorowania zachodzących zdarzeń. Ponadto takie zapisy umożliwiają zwrot kosztów za pomocą obciążenia zwrotnego według różnych stawek dla różnych programów lub dla uruchamiania programów o różnych porach dnia. Co ważniejsze, zapis, które programy zostały wykonane przez kogo iw jakim czasie, może być nieoceniony w badaniach kryminalistycznych.

Zakończenie procesu.

Przeglądając zapis dziennika zakończenia procesu, administrator będzie mógł stwierdzić, kiedy każdy proces został zakończony lub zakończony z innego powodu. Niektóre systemy mogą dostarczać więcej informacji, np. dlaczego wystąpiło nieplanowane lub nagłe zakończenie, ale nie wszystkie zapisy dziennika zakończenia procesu dostarczają tych informacji. Zapisy zakończenia procesu zazwyczaj zawierają cenne informacje statystyczne, takie jak:

* Który proces zrodził lub rozwidlił dany proces

* Identyfikacja wszelkich procesów zrodzonych przez procesy

* Liczba użytych milisekund procesora

* Liczba plików otwieranych i zamykanych przez proces

* Całkowita liczba operacji wejścia/wyjścia (I/O) wykonanych przez proces

* Całkowity rozmiar partycji pamięci przydzielonych procesowi

* Maksymalny rozmiar stosu danych

* Liczba i maksymalny rozmiar dodatkowych segmentów danych w pamięci

* Ile operacji wymiany pamięci wirtualnej było potrzebnych podczas istnienia procesu

* Maksymalny priorytet przypisany procesowi do planowania przez menedżera zadań

Inicjacja sesji.

Sesja składa się z komunikacji między określonym użytkownikiem a określonym serwerem w określonym czasie. Za każdym razem, gdy użytkownik loguje się do systemu i inicjuje sesję, zapis tego zdarzenia można znaleźć w rekordzie dziennika inicjacji sesji. Częste przeglądanie tych zapisów dostarcza ważnych informacji ostrzegających administratorów o obecności intruza w systemie. Na przykład, jeśli administrator wie, że autoryzowany użytkownik jest na urlopie, a plik dziennika inicjowania sesji pokazuje, że sesja została zainicjowana dla tego konkretnego identyfikatora użytkownika, istnieje duże prawdopodobieństwo, że osoba nieupoważniona użyła systemu za pośrednictwem pożyczonego lub skradzionego identyfikatora użytkownika. Zapisy te są szczególnie cenne podczas prac kryminalistycznych.

Zakończenie sesji.

Kiedy sesja kończy się z jakiegokolwiek powodu, kopia czasu jej zakończenia jest zwykle przechowywana w rekordzie dziennika zakończenia sesji. Podobnie jak rekord zakończenia procesu, rekord zakończenia sesji może zawierać wiele zagregowanych informacji o działaniach wykonanych podczas sesji, takich jak całkowita liczba operacji we/wy, całkowita liczba uruchomionych i zakończonych procesów, całkowita liczba otwartych i zamkniętych plików , i tak dalej.

Nieprawidłowe próby logowania.

Plik nieprawidłowej próby logowania może okazać się nieoceniony w przypadkach, gdy próby logowania się nie powiodą. W niektórych przypadkach plik może stwierdzić, czy użytkownik próbował zalogować się przy użyciu nieprawidłowego hasła, czy przekroczył dozwoloną liczbę nieudanych prób lub czy użytkownik próbował zalogować się w pozornie nietypowym czasie. Te zapisy dziennika mogą dostarczyć ważnych informacji w przypadkach, gdy administrator próbuje śledzić określone działania użytkownika lub upewnić się, czy niepowodzenie logowania było spowodowane prostym błędem, czy też próbą podszywania się pod inną osobę z zewnątrz. W sieciach przewodowych, w których każde urządzenie ma unikalny identyfikator, rekordy zwykle zawierają określony identyfikator, który umożliwia administratorom wyśledzenie fizycznego urządzenia użytego do próby logowania.

Plik Otwórz.

Rekord dziennika otwartych plików zawiera informacje o tym, kiedy każdy konkretny plik został otwarty i przez jaki proces; ponadto rekord ogólnie rejestruje tryb, w którym plik został otwarty: na przykład wyłączny odczyt i zapis, wyłączny odczyt, wyłączny zapis z równoczesnym odczytem, tylko dołączanie lub współbieżny odczyt i zapis.

Plik Zamknij.

Rekord dziennika zamknięcia pliku dostarcza administratorowi informacji o tym, kiedy plik został zamknięty, przez jaki proces iw jaki sposób. Plik zwykle przechwytuje informacje o tym, czy użytkownik specjalnie zamknął plik lub czy wystąpił jakiś inny rodzaj przerwy. Rekordy zwykle zawierają szczegółowe informacje na temat wszystkich operacji odczytu i zapisu, w tym liczbę fizycznych blokad przesłanych w celu wykonania całkowitej liczby logicznych operacji we/wy.

Nieprawidłowe próby dostępu do pliku.

Ważny zapis dziennika w działaniu M&C, nieprawidłowa próba dostępu do pliku, pokazuje administratorowi, kiedy i do jakich plików miały miejsce nieprawidłowe próby dostępu do pliku. Rekordy ogólnie pokazują, który proces próbował wykonać operację we/wy i dlaczego został odrzucony przez system plików (np. próba zapisu do pliku otwartego tylko do odczytu, naruszenie listy kontroli dostępu lub naruszenie barier dostępu do plików).

Plik we/wy.

Za każdym razem, gdy informacje są umieszczane, odczytywane lub usuwane z pliku (wejście/wyjście), informacje dotyczące tych zmian są przechwytywane w dzienniku we/wy pliku. Jak wspomniano wcześniej, dziennik zawiera obrazy rekordu przed i po uzyskaniu do niego dostępu. Dziennik we/wy może być używany do odzyskiwania plików po awarii systemu lub aplikacji. W połączeniu z rekordami inicjowania i kończenia transakcji, takie dane mogą być wykorzystywane w systemach automatycznego wycofywania lub przywracania zmian. Zarejestrowane tutaj działania mogą okazać się szczególnie pomocne przy próbie walidacji podjętych działań i przypisania ich do konkretnych osób. Szczegółowe dzienniki są typowe dla baz danych, w których podsystem zapewnia opcjonalne rejestrowanie wszystkich operacji we/wy. Zapisy dziennika aplikacji, zaprojektowane i zaprogramowane przez twórców aplikacji, zazwyczaj umożliwiają administratorom włączenie takiego szczegółowego rejestrowania.

Aktywność konsoli systemowej.

Plik działań konsoli systemowej zawiera informacje o wszelkich akcjach, które pochodzą z konsoli systemowej lub są wyświetlane w konsoli systemowej. Zwykle konsola systemowa zawiera nie tylko rekordy logowania i wylogowywania, ale także żądania specjalne, takie jak podłączenie formularza drukarki, podłączenie określonej taśmy lub kasety, komentarze wysyłane do konsoli przez zadania wsadowe oraz swobodną komunikację od użytkowników. Plik konsoli rejestruje wszystkie takie działania, a także każde polecenie operatora systemu, a system odpowiada na te polecenia. Zapisy te stanowią doskonałe narzędzie dla śledczych do śledzenia określonych zdarzeń w incydencie komputerowym.

Aktywność sieciowa.

Pliki aktywności sieciowej dostarczają cennych informacji na temat aktywności w sieci. W zależności od wyrafinowania i ustawień systemu używanego przez administratora, uzyskane informacje mogą być obfite lub skąpe. Określone urządzenia mogą generować własne rejestry aktywności w sieci; na przykład routery, bramy i zapory mogą przechowywać własne pliki dziennika. Jednakże, zazwyczaj są to pliki obiegowe, w których wpisy do wpisania po zapełnieniu zbioru są przesuwane na początek zbioru, gdzie nadpisują najstarsze wpisy. W pracy kryminalistycznej konieczne jest przechwycenie takich danych, zanim interesujące informacje zostaną zatarte. Niestety w wielu systemach natężenie ruchu sieciowego jest tak duże, że pliki dziennika zawierają tylko ostatnie minuty ruchu.

Utylizacja zasobów.

Przegląd zapisów dziennika wykorzystania zasobów pokaże wszystkie zasoby systemu i poziom wykorzystania każdego z nich. Monitorując ten plik, administratorzy często podejmują ważne decyzje dotyczące modyfikacji konfiguracji systemu lub rozbudowy systemu.

Jednostka centralna.

Plik procesora pokazuje pojemność i wykorzystanie jednostki centralnej dla dowolnego systemu, który jest używany i monitorowany.

Na podstawie tych informacji administratorzy mogą monitorować, kiedy użycie jest największe i procesor jest najbardziej obciążony, i może decydować o zasadach i wymaganiach dotyczących wykorzystania, a także o możliwych aktualizacjach procesora. Podobnie jak w przypadku wszystkich analiz plików dziennika, można zbadać wszelkie wartości odstające (nietypowe wartości) i wszelkie nieoczekiwane zmiany w użyciu. Globalne rekordy wykorzystania procesora można porównać z sumą wykorzystania procesora zebraną z zapisów zakończenia procesu; rozbieżności mogą wskazywać na ukradkowe działanie nieautoryzowanych procesów, np. złośliwego oprogramowania.

Miejsca na dysku.

Rekordy dziennika dotyczące miejsca na dysku pokazują ilość miejsca na dysku pierwotnie dostępną w systemie, ilość wykorzystanego miejsca na dysku (i ogólnie, jakiego typu pliki są używane) oraz ilość wolnego i dostępnego miejsca na dysku. Porównanie całkowitego wykorzystania miejsca na dysku z całkowitym miejscem przydzielonym wszystkim plikom może ujawnić problemy, takie jak utracone miejsce na dysku (tj. sektory dysku mają być w rzeczywistości wolne). Takie nieprzydzielone sektory lub klastry mogą również stanowić miejsce, w którym złoczyńcy ukrywają dane, które przechowują bez autoryzacji, omijając system plików.

Zużycie pamięci.

Z zapisów dziennika zużycia pamięci można uzyskać ważne informacje na temat ilości pamięci w systemie oraz ilości faktycznie wykorzystywanej. Takie rekordy zazwyczaj zawierają również informacje o wykorzystaniu pamięci wirtualnej. W związku z tym mogą ostrzegać o warunkach pobicia, w których segmenty pamięci są zbyt często kopiowane na dysk i odczytywane z dysku. Szczegóły zużycia pamięci mogą być przydatne w śledzeniu nieautoryzowanych procesów jak robaki.

Poziom systemu a poziom zadania.

Mogą mieć miejsce różne poziomy monitorowania, rejestrowania i audytu. Niektóre z nich mogą być wstępnie zaprogramowane, ale w większości środowisk możliwe jest wybranie żądanych zapisów dziennika i powiązanych raportów. Na przykład regularny dziennik kontroli na poziomie systemu może być tworzony w określonych odstępach czasu, aby dostarczyć informacji, że system działa bez żadnych nadzwyczajnych problemów. Jednak dogłębny audyt na poziomie stanowiska może odbywać się częściej w celu monitorowania konkretnego zadania i upewnienia się, że działa ono prawidłowo i dostarcza potrzebnych informacji.

Automatyzacja i alokacja zasobów.

Wykorzystanie bezpiecznych, dobrze zorganizowanych systemów zarządzania dziennikami do monitorowania zdarzeń i reagowania na nie może zmniejszyć nakład pracy administracyjnej wymaganej do zarządzania infrastrukturą. Wraz z rosnącymi wymaganiami dotyczącymi zgodności i kosztami związanymi z przechowywaniem danych, ważne jest uwzględnienie zarządzania logami w

zakresie polityki przechowywania danych przedsiębiorstwa. Przepisy dotyczące e-discovery i analiza pośmiertna ataku opierają się na skutecznym dostępie do dokładnych informacji dziennika. Dzienniki wymagają zasobów systemowych, począwszy od przechowywania nośników po cykle procesora i wykorzystanie pamięci. Odkładając potencjalne zasoby biznesowe na potrzeby rejestrowania i raportowania, należy wziąć pod uwagę kompromisy. Ręczne przeglądanie milionów plików dziennika w różnych systemach, w różnych strefach czasowych iw niespójnych formatach jest dla personelu nierealne. W przypadku witryn rozproszonych geograficznie przesyłanie dziennika w czasie rzeczywistym może być opóźnione ze względu na ograniczoną przepustowość wolnych łączy.

Nie wszystkie zarejestrowane informacje mają taką samą wartość. Niektóre rekordy danych mogą być bezpośrednio powiązane z kwestiami zgodności, podczas gdy inne zapewniają niekrytyczne korzyści w codziennej działalności. Na podstawie polityki kierownictwo musi określić, jakie rodzaje danych należy agregować i redukować w celu monitorowania i zapewnienia ciągłej zgodności. Jest to część procesu definiowania zakresu systemów M&C. Planiści i realizatorzy muszą nie tylko określić aktualne wymagania, ale muszą zapewnić, że plan zarządzania dziennikami będzie skalowany w celu zaspokojenia postrzeganego zapotrzebowania na zasoby w zakresie wymagań operacyjnych, bezpieczeństwa i zgodności.

Bezpieczeństwo rekordów dziennika.

Organizacja musi chronić swoje zapisy w dzienniku przed nieautoryzowanym dostępem i modyfikacją. Cztery najczęstsze metody zabezpieczania rekordów dziennika to: listy kontroli dostępu, sumy kontrolne, szyfrowanie i podpisy cyfrowe. Połączenie tych metod, w oparciu o wymagania systemowe, może odpowiednio zabezpieczyć większość danych dziennika. Atakujący z nieskrępowanym dostępem do niezaszyfrowanych plików dziennika poczty e-mail mogą pobierać kopie plików i wyszukiwać w nich poufnych informacji oraz modyfikować lub usuwać treść wiadomości bezpośrednio z serwera docelowego. Ten typ ataku zagraża każdemu elementowi heksady Parkera. Oprócz powszechnych obaw związanych z naruszeniem poufności i utratą integralności danych, nieautoryzowany dostęp do plików dziennika może dostarczyć atakującemu dodatkowych informacji o środowisku sieciowym. Skanery luk w zabezpieczeniach mogą działać w zaplanowanych odstępach czasu i rejestrować wykryte problemy w centralnej bazie danych. Wykorzystując zagregowane dane, osoba atakująca może skuteczniej naruszyć środowisko sieciowe i ominąć procedury wykrywania przyzwyczajone do rozpoznania o dużym obciążeniu. System operacyjny i listy kontroli dostępu na poziomie aplikacji (ACL) ograniczają dostęp do plików. Niektóre pliki dziennika mogą być zapisywane na nośnikach jednokrotnego zapisu i wielokrotnego zapisu (WORM) dla audytorów lub personelu prawnego. Personel operacyjny może nie mieć uzasadnionej potrzeby dostępu do takich danych. Jednak może być konieczne zapewnienie ciągłego przepływu komunikacji. Bazy danych mogą wdrażać jeszcze bardziej szczegółowe kontrole określonych rekordów i pól, aby uniknąć niepotrzebnego ujawniania informacji. Podczas planowania systemu M&C dla danych dziennika należy również wziąć pod uwagę fizyczne kontrole dostępu do nośnika podczas przechowywania lub transportu. Prawidłowo zaimplementowane listy ACL mogą ograniczyć poziom narażenia danych dziennika na upoważniony personel i procesy systemowe. Organizacje podlegające PCI DSS są zobowiązane do wdrożenia kontroli integralności danych dziennika. W przeszłości 32-bitowe cykliczne kontrole redundancji (CRC) generowały sumy kontrolne w celu ochrony przed zmianami w plikach. Obecnie silniejsze kryptograficzne sumy kontrolne, takie jak te generowane przez rodzinę SHA-2, zapewniają bardziej rozsądny poziom pewności. Sumy kontrolne nie wymagają stałej interakcji człowieka. W celu ochrony przed manipulacją system monitorowania może stanowić punkt odniesienia dla systemu i przechowywać kopie plików lub ich odpowiedniki skrótów w celu okresowego porównywania plików lub w czasie rzeczywistym. Zmiany w dziennikach lub innych krytycznych plikach można następnie

centralnie zgłaszać w celu ręcznego zbadania. System kontroli może automatycznie poddać kwarantannie nieautoryzowany plik i przywrócić kopię oryginalnego pliku. Podpisy cyfrowe wykorzystują kryptografię klucza publicznego w celu zapewnienia integralności i niezaprzeczalności danych. Opierają się one na standardowych kryptograficznych sumach kontrolnych, ponieważ nie tylko potwierdzają integralność plików, ale także identyfikują, kto lub jaki podmiot zapewnia to zapewnienie. W przypadku organizacji, które muszą przesyłać raporty odbiorcom zewnętrznym, takim jak urzędy państwowe, podpisy cyfrowe mogą skrócić drogę papierową i zapewnić wydajniejszy, cyfrowy sposób spełnienia wymagań prawnych. Szyfrowanie należy wziąć pod uwagę w przypadku danych dziennika podczas przesyłania i w stanie spoczynku. Szyfrowanie całych plików dziennika ogranicza możliwość przeglądania lub modyfikowania zawartości. Zwiększa również wykorzystanie zasobów w systemie docelowym podczas procesu szyfrowania. Podobnie jak sumy kontrolne, klucze wymagane do odszyfrowania powinny być przechowywane w bezpiecznym miejscu, aby zwiększyć trudność w pokonaniu kontroli. Korzystanie z szyfrowania całego dysku, a następnie przesyłanie pliku dziennika przez sieć w postaci zwykłego tekstu nie jest spójną metodą zabezpieczania dziennika. Ustanawianie bezpiecznych łączy sieciowych, takich jak wdrażanie protokołu IPSec, zapewnia kompleksowe bezpieczeństwo łącza. Do prawidłowego zabezpieczenia plików dziennika i innych poufnych informacji może być konieczne połączenie szyfrowania na poziomie sieci i systemu. Planując system zarządzania logami, należy również wziąć pod uwagę łańcuch dostaw. Niektóre dane dziennika mogą wymagać wykorzystania w sądzie. Bez weryfikowalnej ścieżki audytu treść może być niedopuszczalna. Udokumentowany łańcuch dowodowy dla transferów mediów między personelem a lokalizacjami może potwierdzić kontrolę fizyczną. Implementacja łańcuchów bloków szyfrowania (CBC) może dodatkowo chronić przed nieautoryzowanymi zmianami danych dziennika. Tekst zaszyfrowany poprzedniego pliku dziennika zawierał Exclusive-Or (XOR) z bieżącym tekstem jawnym, aby utworzyć nową wartość dla operacji szyfrowania. Ta koncepcja może być również przydatna do zapisu zestawów w plikach dziennika i aplikacjach bazodanowych, ponieważ będzie identyfikować usunięcia rekordów i inne modyfikacje danych.

OGÓLNE ZAJĘCIA Z LOGOWANIA

Działania M&C różnią się w zależności od zakresu biznesowego, celów i docelowych funkcji systemu. Cele można pogrupować w ogólne klasy, w tym: przebieg procesu, planowanie zadań, łączność sieciowa, pomiary środowiskowe, zapewnienie stanu systemu, stan komponentów systemu, działania procesu, ustawienia konfiguracji, informacje o systemie plików i kontrola dostępu. Obecne przepisy mogą obejmować tylko podzbiór systemów informatycznych organizacji w zakresie zgodności. Zmiany w infrastrukturze i wymaganiach dotyczących zgodności są nieuniknione. Ważne jest wdrożenie skalowalnego i elastycznego M&C, aby sprostać przyszłym potrzebom.

Przepływ procesów i planowanie zadań.

Niektóre organizacje używają kombinacji zasobów systemu mainframe i rozproszonego. Grupa komputerów mainframe może używać określonego harmonogramu zadań wsadowych do przetwarzania i monitorowania stanu zadań i danych wyjściowych. Inne systemy rozproszone w całej organizacji mogą korzystać z własnych harmonogramów i funkcji rejestrowania. Złożoność tego projektu nie ułatwia jednak monitorowania i audytu w całym przedsiębiorstwie. Scentralizowany harmonogram zadań może być niezbędny do monitorowania i kontrolowania przepływu zadań. Scentralizowany system będzie musiał łączyć się z różnymi systemami w celu zbierania statusu zadań i inicjowania poleceń. Dla kierownictwa korporacyjny pogląd na planowanie zadań może zidentyfikować niepotrzebną złożoność i nadmiarowość, prowadząc do przyszłego doskonalenia procesów. W przypadku przejścia na centralny system planowania zadań może się wydawać pożądane natychmiastowe przeniesienie całego środowiska lub przywrócenie centralnego komputera typu

mainframe. Jednak stopniowa migracja do scentralizowanej M&C byłaby bardziej idealną metodą zmiany.

Łączność sieciowa.

Łączność sieciowa odnosi się do protokołów urządzeń i mediów komunikacyjnych (przewodowych lub bezprzewodowych) używanych w środowisku komputerowym. Centrum operacji sieciowych będzie chciało monitorować stan łączy sieciowych, wskaźniki stanu krytycznych urządzeń i strumienie danych przechodzące przez sieć. W środowisku warstwowym fizyczny dostęp do okablowania sieciowego może być zabezpieczony w torach kablowych i szafach sieciowych lub w punktach dystrybucji. Urządzenia będą aktualne i skonfigurowane zgodnie z najlepszymi praktykami. Niepotrzebne protokoły będą kontrolowane poprzez blokowanie lub kierowanie podejrzanego ruchu do sieciowych czarnych dziur i sieci miodu w celu dalszej analizy. Sieciowe systemy zapobiegania włamaniom (IPS) mogą identyfikować anomalie komunikacyjne, blokować wymianę komunikacyjną, rejestrować zdarzenia i wyzwalać alert administracyjny. Zapobieganie wymaga planowania i wystarczających kontroli, aby uniemożliwić atakowi osiągnięcie jego celu. Metoda implementacji M&C dla wrażliwych węzłów sieciowych może obejmować przenoszenie węzłów do odizolowanych segmentów, wdrażanie sieciowych IPS w linii i wykorzystywanie agentów bezpieczeństwa opartych na hoście. Dodatkowe narzędzia do oceny bezpieczeństwa przedsiębiorstwa mogą również skanować, raportować, generować zgłoszenia, proponować środki zaradcze i analizować trendy bezpieczeństwa w czasie. Oprócz monitorowania ogólnej łączności sieciowej, niektóre sieci są specjalnie wdrażane na potrzeby M&C. Starsze systemy przemysłowe integrują teraz typowe elementy sieci Ethernet w środowiskach mechanicznych, elektromechanicznych i elektronicznych. Dostępne są również bezprzewodowe opcje M&C. Specyfikacja ZigBee wykorzystuje standard IEEE 802.15.4 do zapewniania łączności sieci lokalnej ad hoc. ZigBee jest używany głównie w M&C. W hali produkcyjnej lub obiekcie zewnętrznym dodatkowe okablowanie dla systemów M&C może być niewykonalne. Potencjalnym rozwiązaniem może być integracja niedrogich, solidnych punktów kontrolnych ZigBee. W przypadku lokalizacji rozproszonych geograficznie, usługi bezpiecznych połączeń o dużej przepustowości, takie jak połączenia satelitarne, łącza dzierżawione i sieci wirtualnej prywatnej (VPN), łączą lokalizacje w celu centralnego zarządzania danymi M&C.

W zakresie ochrony środowiska.

Niektóre zmienne środowiskowe są łatwiejsze do monitorowania niż kontrolowania. Niezależnie od tego, czy używamy ZigBee do przesyłania informacji sensorycznych, czy pakietu oprogramowania do pomiaru nieregularności napięcia AC, środki ochrony środowiska zapewniają dodatkową świadomość sytuacyjną dla systemów informatycznych i personelu. Wilgotność, temperatura, dym i wyciekająca woda mają bezpośredni wpływ na systemy komputerowe w centrum danych. Dedykowane klimatyzatory i osuszacze mogą monitorować i kontrolować wilgotność i temperaturę. Nieokreślone źródła dymu lub wycieku wody mogą być trudne do kontrolowania za pomocą zautomatyzowanej reakcji, ale monitorowanie i powiadamianie o alarmie mogą wywołać procedury naprawcze ze strony personelu w celu ograniczenia ryzyka. Czynniki środowiskowe mogą również wpływać na jakość produktów organizacji. M&Csystems może usprawnić wysiłki organizacji w zakresie kontroli jakości, zapewniając spójne wytwarzanie produktów w ramach predefiniowanych tolerancji. W ramach planu ciągłości biznesowej może okazać się konieczne, aby organizacja monitorowała i przygotowywała się na zagrożenia środowiskowe, takie jak powodzie, zawalenie się konstrukcji i utrata zasilania. System monitorowania z funkcją wczesnego ostrzegania mógłby powiadamiać personel o konieczności zgłoszenia się do alternatywnego miejsca pracy lub przygotowania się do działań awaryjnych. W przypadku, gdy zagrożenie środowiskowe zakłóci działanie systemów sterowania, personel musi mieć możliwość ręcznego sterowania. EPA zaleca znajomość operacji ręcznych, w przypadku awarii systemu

nadzoru i akwizycji danych (SCADA). Oprócz ręcznego sterowania, integracja redundantnych systemów M&C z bezproblemowym przełączaniem awaryjnym może zmniejszyć prawdopodobieństwo zakłóceń operacyjnych.

Stan systemu.

Stan systemu odnosi się do zbioru krytycznych zmiennych w systemie docelowym. System monitorowania może wymagać śledzenia uruchomionych procesów w pamięci, usługach, otwartych połączeniach portów, plikach systemowych, stanie sprzętu i danych dziennika. W przemysłowych systemach sterowania stan systemu może odzwierciedlać ogólny obraz sieci elektrycznej lub ograniczać się do tego, czy zestaw zaworów jest otwarty, czy zamknięty. Gdy proces aplikacji antywirusowej nie uruchamia się, co skutkuje późniejszą infekcją złośliwym oprogramowaniem, system monitorowania może wywołać alert, aby personel lub zautomatyzowany system kontroli mógł wyizolować infekcję. Jedną z metod monitorowania stanu systemu jest uruchomienie agenta w systemie hosta. Agenci programowi monitorują wstępnie zdefiniowaną listę elementów i regularnie zgłaszają stan do centralnego centrum monitorowania. Gdy agent nie odpowiada lub „zameldowuje się", system monitorowania może wysłać alert w celu zbadania problemu. Systemy zapobiegania włamaniom hosta (HIPS) chronią stan systemu węzłów w środowisku sieciowym. System HIPS analizuje działania w oparciu o procedury wykrywania sygnatur i heurystyki. Zapewniają rozsądne środki monitorowania i kontroli (M&C), z możliwością scentralizowanego raportowania i korelacji ataków. W przypadku analizy pośmiertnej zrzuty pamięci mogą być przydatne w analizie problemów ze stanem systemu. Jeśli system monitorowania sieci wykrył aktywność związaną z botnetem pochodzącą z systemu w zasobach ludzkich, przechwycenie aktualnego stanu systemu może być korzystne dla dochodzenia. W ramach procesu zbierania dowodów w kryminalistyce kontrolowanie i zachowanie stanu systemu wymaga specjalistycznego szkolenia i narzędzi

Komponenty systemu

Aplikacje monitorujące mogą śledzić wykorzystanie i ogólną wydajność komponentów systemu, w tym procesora, pamięci i nośników pamięci. Systemy operacyjne mają również wbudowane narzędzia do monitorowania komponentów i przechowywania wyników w plikach dziennika. Systemy zarządzania zapasami zbierają informacje na poziomie komponentów, a także informacje o oprogramowaniu skonfigurowane przez personel operacyjny. Sześć miesięcy po odświeżeniu sprzętu audyt może zidentyfikować systemy działające tylko z połową pierwotnie zakupionej pamięci. Zarejestrowane informacje pomogą określić zakres problemu. Monitorowanie wydajności komponentów systemu może również identyfikować zmiany w potrzebach biznesowych lub nadużycia systemu. Wraz z wdrożeniem nowego portalu internetowego istniejące serwery proxy sieci Web mogą nie być już w stanie obsłużyć większego obciążenia. Zarejestrowane dane dotyczące wydajności potwierdziłyby potrzebę rozbudowy infrastruktury lub zwiększenia pojemności istniejących systemów. Nastawy wydajności wyzwalają alerty, gdy podzespoły odbiegają od normalnego poziomu działania. Alerty mogą identyfikować zmiany wywołane zewnętrznie, takie jak spadki napięcia lub wewnętrzne ograniczenia, takie jak maksymalne wykorzystanie pamięci. Wysokie wykorzystanie zasobów na historycznie bezczynnym komputerze PC z interfejsem HMI może nawet wskazywać na niewłaściwe użycie systemu do działań niezwiązanych z SCADA, takich jak skanowanie sieci wewnętrznej, narzędzia do łamania haseł lub gry. Monitory komponentów systemu najczęściej próbują zidentyfikować nadmiernie obciążone procesory, duże zużycie pamięci i pełne nośniki pamięci. Jednak identyfikacja rutynowo niewykorzystywanych zasobów daje kierownictwu możliwość realokacji zasobów do obszarów potrzeb zamiast zakupu niepotrzebnych dodatków do infrastruktury. Przydziały dysku kontrolują dozwoloną ilość nośników użytecznych dla użytkowników i aplikacji. Aby chronić system przed niezamierzonym lub złośliwym nadmiernym wykorzystaniem, przydziały powinny być

przeglądane w ramach strategii warstwowej. Maszyny wirtualne wykorzystują do sterowania przydziały pamięci masowej, pamięci i procesora zasobów wykorzystywanych w systemie hosta. W przypadku dużych środowisk wirtualizacji może być niezbędny system menedżera wirtualnego przedsiębiorstwa, aby zapewnić odpowiednie równoważenie obciążenia na wszystkich hostach systemu wirtualnego, a także określić, czy wymagane jest dodatkowe dostrojenie w celu poprawy wydajności maszyny wirtualnej.

Działania procesowe

Proces odnosi się do działającego programu w urządzeniu komputerowym. Procesy mogą być inicjowane na poziomie systemu lub użytkownika i mogą zawierać wiele wątków. Procesy M&C mogą zapobiegać infekcjom złośliwym oprogramowaniem i identyfikować nieprawidłowe działania procesów. Systemy antywirusowe zazwyczaj zajmują się tym obszarem. Robak SQL Slammer atakował podatny na ataki proces przez połączenie sieciowe, wstrzykując kod do pamięci bez zapisywania na dysku16. Oprócz monitorowania procesów, analiza ruchu sieciowego i sieciowe systemy IPS mogą ograniczać tego typu działania. Korzystanie z narzędzi do monitorowania przedsiębiorstwa w celu agregowania krytycznych informacji o procesach w wielu systemach pomoże zidentyfikować problemy z aplikacjami, takie jak niekontrolowane procesy. W celu dostrajania wydajności i oceny zasobów agenci mogą również monitorować czas pracy procesora uruchomionych programów pod kątem wysokiego wykorzystania. Monitorowanie działań procesowych może również odgrywać rolę w pomiarach oprogramowania i raportowaniu. Organizacje mogą chcieć identyfikować wykorzystanie aplikacji przez różne działy, aby uniknąć wdrażania niepotrzebnych aplikacji i płacenia opłat licencyjnych za półki. Agenci mogą centralnie raportować czas, który upłynął dla procesów docelowych, agregacji danych i generowania raportów zarządczych. Monitorowanie użycia określonych typów oprogramowania narzędziowego, na przykład używanych głównie przez personel administracyjny i bezpieczeństwa (np. nmap, tcpdump, hping, Wireshark i Microsoft SysInternals), może również wskazywać na nieautoryzowane rozpoznanie sieci. Blokowanie wykonywania znanych aplikacji za pomocą nazwy pliku lub wartości skrótu może ograniczyć poziom działań następczych wymaganych do zlokalizowania i zabicia zdalnych procesów. Monitorowanie niesklasyfikowanych lub niezatwierdzonych procesów może dodatkowo pomóc w zidentyfikowaniu przyczyny spadku wydajności w systemach zdalnych.

System plików

Działania systemu plików dostarczają wielu informacji kontrolnych. Systemy plików przechowują dane dziennika, od błędów aplikacji po nieautoryzowane próby uwierzytelnienia. Podobnie jak rejestrowanie IDS, rejestrowanie systemu plików wymaga dostrojenia wydajności w celu agregowania danych i uniknięcia utraty danych. Rejestrowanie każdej próby dostępu do pliku i modyfikacji danych w systemie spowoduje zapełnienie dzienników zdarzeń ogólnie bezużytecznymi informacjami. Jeśli właściciele systemów skonfigurują plik dziennika tak, aby po zapełnieniu był zastępowany, rzeczywiste zdarzenia krytyczne mogą zostać utracone. Liczba wpisów w dzienniku ma również wpływ na zasoby sieciowe. Ciągły przepływ dzienników aktywności systemu plików może negatywnie wpłynąć na wydajność modułu zbierającego dzienniki. Skoncentrowanie się na krytycznych plikach systemowych, wrażliwych danych i ustawieniach konfiguracji zmniejszy liczbę wpisów w dzienniku i zapewni bardziej ukierunkowany zestaw wyników. Pliki konfiguracyjne systemów operacyjnych i aplikacji wymagają warstw ochrony, aby uniknąć nieautoryzowanych modyfikacji. Podobnie jak warstwy omówione w podrozdziale 53.3.4, dotyczące bezpieczeństwa rekordów dziennika, listy kontroli dostępu (ACL), szyfrowanie, podpisy cyfrowe i sumy kontrolne mogą odgrywać kluczową rolę w ochronie obiektów w systemie plików. Próby obejścia systemów M&C mogą rozpocząć się od plików konfiguracyjnych i ustawień. Użytkownicy końcowi próbujący ominąć filtry InternetWeb mogą ponownie skonfigurować

swoje przeglądarki internetowe, aby korzystały z fałszywego serwera proxy. Atakujący próbujący zmodyfikować konfigurację słabo zabezpieczonego serwera sieci Web mogą wykorzystać luki w zabezpieczeniach do zaatakowania dodatkowych systemów podłączonych do sieci wewnętrznej. Kontrolowanie zmian w ustawieniach konfiguracyjnych za pomocą zasad systemowych i systemu HIPS ograniczy tego rodzaju ataki.

Kontrola dostępu

Kontrola dostępu jest centralną częścią działań związanych z zarządzaniem bezpieczeństwem i zapewnianiem zgodności. Organizacje często polegają na więcej niż jednym autonomicznym systemie identyfikacji i uwierzytelniania, w tym aplikacji, sieciowych systemów operacyjnych i bezpieczeństwa budynków. W rezultacie stają przed poważnymi wyzwaniami podczas próby komunikowania się, agregowania i zarządzania zdarzeniami kontroli dostępu. Dodawanie i usuwanie personelu w bezpiecznym środowisku może wiązać się z identyfikacją identyfikatora, tokenami bezpieczeństwa i hasłami. System M&C ukierunkowany na kontrolę dostępu będzie musiał zapewnić, że nieupoważniony personel nie będzie miał dostępu do żadnych zasobów fizycznych ani cyfrowych. Kierownictwo może najpierw potrzebować opracować przebieg procesu przy wsparciu personelu operacyjnego i interesariuszy biznesowych. Agregowanie dzienników dostępu i wyszczególnianie nieudanych prób logowania oraz wielu wystąpień użytkowników pomaga w identyfikacji nadużyć systemu. Gdy użytkownicy logują się do zasobów sieciowych, ustanawiają sesję z systemem docelowym. Wiele sesji dla tego samego użytkownika w wielu witrynach może oznaczać, że konto użytkownika zostało przejęte lub jest udostępniane. W zależności od poziomu ważności informacje te mogą pojawić się w raporcie o wyjątkach, wywołać alert administracyjny lub spowodować automatyczną blokadę konta. Podobnie seria nieudanych prób logowania może osiągnąć próg i automatycznie wyłączyć konto użytkownika na określony czas. Ta kontrola minimalizuje wysiłek wymagany do aktywnego monitorowania kont systemowych, zapewniając jednocześnie, że osoby atakujące nie będą w stanie przeprowadzić ataku siłowego na dane uwierzytelniające autoryzowanego użytkownika.

AGREGACJA I REDUKCJA DANYCH

Scentralizowane magazyny danych.

Systemy generują logi w różnych formatach, do których dostęp nie zawsze jest łatwy. Pierwszą fazą agregacji danych jest upewnienie się, że logowanie działa poprawnie w systemie docelowym. Może to wymagać instalacji dodatkowego oprogramowania do zbierania dzienników w celu wypychania lub pobierania danych w standardowym formacie syslog. Druga faza, polegająca na stopniowym łączeniu punktów rejestrowania ze scentralizowanym magazynem danych, opiera się na indywidualnych mechanizmach rejestrowania w celu stworzenia korporacyjnego widoku zdarzeń. Scentralizowane przechowywanie danych zapewnia pojedynczy punkt analizy i audytu, bez czasochłonnego procesu ręcznego sprawdzania poszczególnych systemów w całym środowisku. Dane dziennika muszą być przekazywane w bezpieczny sposób. System oparty na agentach musi ustanowić bezpieczny kanał komunikacji z głównym kolektorem, aby uniknąć przekazywania szczegółów dziennika do nieautoryzowanego kolektora. Korzystne może być również zakazanie agregatorowi dzienników gromadzenia niechcianych komunikatów syslog. Ten środek bezpieczeństwa może być wbudowany w mechanizm przekazywania lub agregacji dzienników albo może wykorzystywać protokół IPSec przez kontrolowane łącza sieciowe. Głównym problemem związanym z magazynami danych o dużej objętości jest czas przetwarzania. Przetwarzanie dziennika może potencjalnie opóźnić lub w inny sposób uniemożliwić reakcję na incydent. W zależności od dostępnych zasobów ekonomicznie bardziej opłacalne może być przechowywanie zabezpieczonych danych dziennika w skompresowanych

archiwach przy jednoczesnym korzystaniu z monitorowania opartego na agentach wyłącznie w celu zgłaszania krytycznych problemów bezpieczeństwa lub problemów operacyjnych do centralnego magazynu. Czas i wysiłek potrzebny na rejestrowanie, analizowanie i raportowanie każdego bloku danych otrzymanego przez centralny kolektor może przekraczać wymagania wewnętrznej polityki bezpieczeństwa i postrzegane korzyści finansowe. Odfiltrowywanie niekrytycznych zdarzeń i alertów byłoby wówczas częścią podstawowego procesu centralnego systemu M&C. Przechowywanie i analizowanie całych plików dziennika może służyć jako dodatkowy (wolniejszy) mechanizm monitorowania, podczas gdy alerty dotyczące bezpieczeństwa są obsługiwane natychmiast.

Filtrowane zapytania

Ilość zapisów w plikach dziennika może być przytłaczająca i generalnie niemożliwa do indywidualnego i regularnego przeglądania przez personel operacyjny. Centralne przechowywanie danych nie zmienia niewykonalności zadania. Pozwala to jednak na lepszą redukcję danych. Przekształcenie surowych danych w sensowną, zredukowaną formę może zminimalizować szum i umożliwić personelowi oraz zautomatyzowanym procesom ukierunkowanie działań o wyższym priorytecie. Uruchamianie filtrowanych zapytań względem rekordów dziennika może zapewnić szybsze wyniki w przypadku potencjalnych ataków lub problemów systemowych. Zaplanowana kwerenda może zawierać listę wszystkich nieudanych prób logowania. Dodatkowe filtrowanie może obejmować zestaw zasobów obliczeniowych (np. serwery przetwarzające dane kart kredytowych) lub typy użytkowników, takie jak konta administratora. Inne, bardziej szczegółowe zapytanie może zawierać jedynie listę anomalii w ruchu sieciowym między działem badań i rozwoju a szeregiem internetowych serwerów proxy.

Analizowanie zapisów dziennika

Zapisy dziennika mogą być cenne dla administratora systemu, ale tylko wtedy, gdy są używane. Właściwe korzystanie z pliku dziennika wymaga monitorowania i przeglądania jego zapisów, a następnie podejmowania działań na podstawie ustaleń. Taka analiza zazwyczaj wykorzystuje narzędzia dostarczane przez dostawcę systemu operacyjnego lub strony trzecie, takie jak komercyjne firmy produkujące oprogramowanie lub dystrybutorzy bezpłatnego oprogramowania.

Rozważania dotyczące objętości

Ktoś musi podjąć decyzję, jak duże powinny być pliki dziennika. Taka decyzja jest zwykle podejmowana przez administratora systemu i opiera się na tym, co uważa się za przydatne i wykonalne. Jeśli w grę wchodzą pieniądze — na przykład, jeśli potrzebna jest dodatkowa pojemność pamięci masowej — dyrektor techniczny (CTO), dyrektor ds. do udziału w procesie decyzyjnym. Jednak w ciągu trzech i pół dekady, od 1980 r. do czasu pisania tego tekstu w czerwcu 2013 r., koszty miejsca na dysku spadły o około 37 procent rocznie — z około 853 000 USD za gigabajt (w dolarach z 2013 r.) do około 0,04 USD za gigabajt w 2013 r. stałe dolary, więc miejsce na dysku nie stanowi już większego problemu.17 Ważniejsze jest to, że pliki dziennika, jak każdy plik, mogą pozostać w niespójnym stanie w przypadku awarii systemu; zamknięcie pliku dziennika i otwarcie nowego pliku z serii to środek zapobiegawczy, który gwarantuje, że mniej informacji zostanie utraconych w dyskowych buforach I/O w przypadku awarii systemu. Ponadto rozsądne jest umieszczanie plików dziennika na osobnym dysku kontrolowanym przez oddzielny procesor; w ten sposób można wyłączyć zapis z opóźnieniem (zapisy opóźnione) i wymusić zakończenie operacji we/wy dla każdego rekordu pliku dziennika.

Archiwizacja plików dziennika

Archiwizacja jest bardzo ważną częścią tworzenia i używania plików dziennika. Każda organizacja musi zdecydować, jak długo przechowywać swoje pliki dziennika i gdzie je przechowywać. Decyzje tego

rodzaju są czasami podejmowane w oparciu o względy przestrzenne, ale częściej są podejmowane w oparciu o wymogi prawne w określonych branżach. Niektóre firmy mogą zdecydować się na przechowywanie materiałów przez rok lub dwa, podczas gdy inne mogą być prawnie zobowiązane do przechowywania zarchiwizowanych plików dziennika przez siedem lub osiem lat. Decyzje dotyczące archiwizacji plików logów nigdy nie powinny być podejmowane arbitralnie; w każdym przypadku należy przeprowadzić staranny przegląd i kontrolę wymagań firmowych, prawnych i branżowych. W oparciu o wyniki tego przeglądu należy stworzyć pisemną politykę i procedury. Każda organizacja musi poinformować swoich pracowników, jakie są te zasady i procedury, aby wiedzieli, jakie materiały są przechowywane, gdzie można je znaleźć i jak można uzyskać do nich dostęp.

Programy specyficzne dla platformy do analizy plików dziennika

Istnieje wiele systemów operacyjnych i chociaż istnieją pewne podobieństwa w sposobie ich działania, istnieją również różnice. Może być konieczne specjalne przeszkolenie w zakresie każdego konkretnego systemu operacyjnego w celu przeprowadzenia prawidłowej analizy plików dziennika specyficznych dla platformy generuje.

Raporty o wyjątkach

Ilość rekordów plików dziennika może być przytłaczająca. Na przykład portal bankowy skierowany do klienta może generować wpisy dziennika dotyczące logowania, wylogowań, transakcji finansowych i innych zmian rekordów. Może również rejestrować próby penetracji zabezpieczeń aplikacji sieci Web lub wykrywania przechwyconych sesji bankowych. Raporty o wyjątkach pozwalają analitykowi skupić się na określonych cechach (np. nietypowych przelewach bankowych do innych krajów). Takie narzędzia znacznie upraszczają wykrywanie i analizę anomalii oraz są szczególnie pomocne w śledzeniu nieautoryzowanych i niepożądanych działań.

POWIADOMIENIA I RAPORTOWANIE

Alerty

Zarządzanie dziennikami musi obejmować warstwy automatyzacji, aby skrócić czas potrzebny do przeglądania zdarzeń w środowisku i reagowania na nie. Sposób, w jaki system M&C radzi sobie z alertami, będzie miał bezpośredni wpływ na bezpieczeństwo systemu docelowego. Przeciążenie operatorów zbyt dużą liczbą alertów spowoduje wydłużenie czasu reakcji na problem, a także potencjalne zignorowanie problemów krytycznych. Celem alertów jest poprawa reakcji na główne problemy, takie jak nieszczelny potok lub awaria sieci w wielu lokalizacjach. Alerty można skonfigurować w określonych punktach, tak aby osoba reagująca była powiadamiana tylko wtedy, gdy próg ataku zostanie osiągnięty. Elementy kontrolowane w środowisku mogą mieć wyższy próg powiadamiania o alertach. Nagły napływ złośliwego oprogramowania z Internetu może zostać natychmiast wykryty i przefiltrowany na brzegu sieci. Powiadomienie personelu operacyjnego o dużej ilości złośliwego oprogramowania może być przydatne. Jednak spamowanie administratorów bezpieczeństwa alertami o każdym zablokowanym ataku byłoby nieefektywnym wykorzystaniem zasobów powiadomień o alertach. Ponadto środki powiadamiania o alertach odgrywają ważną rolę w ciągłości biznesowej i odtwarzaniu po awarii. Systemy monitorowania poza pasmem mogą wykryć błąd sprzętu sieciowego, który w innym przypadku nie mógłby zostać wykryty przez samo uszkodzone urządzenie. Odbiorcy ostrzeżeń mogą potrzebować wielu sposobów powiadamiania. E-mail, pager, telefon komórkowy i wiadomości SMS to najczęstsze formy. Wizualizacja alertów to kolejny cenny sposób dla operatorów aktywnie monitorujących środowisko. Podobnie jak w przypadku deski rozdzielczej, wizualizacja może zredukować dane zebrane z czujników do wizualnej mapy ze wskaźnikami graficznymi do identyfikowania problemów systemowych. Połączenie monitorowania

alertów w stylu pulpitu nawigacyjnego i ukierunkowanego dostarczania wiadomości może zapewnić najlepsze pokrycie problemów o dużym znaczeniu. W środowiskach przemysłowych operatorzy wykorzystują narzędzia HMI do utrzymania świadomości sytuacyjnej z urządzeniami polowymi. Interfejs HMI wykorzystuje wirtualne przyciski i inne elementy wizualne w celu uproszczenia funkcji przemysłowych. Jeśli alerty są często generowane dla działań niekrytycznych, personel wyczyści listę alertów i z czasem je zignoruje. Ignorowanie alertów dotyczących krytycznych problemów może bezpośrednio wpłynąć na produkcję i prowadzić do kosztownych napraw. W tej sytuacji pulpit nawigacyjny zarządzania może wyświetlać statystyki wydajności, które mogą zainicjować dochodzenie w terenie w celu ustalenia pierwotnej przyczyny spadków wydajności produkcji.

Analiza trendów i raportowanie

Agregacja danych, redukcja i korelacja stanowią podstawę analizy trendów. Dane związane z wymogami zgodności mogą być analizowane w celu określenia tempa poprawy bezpieczeństwa w organizacji. Dalsza analiza może określić poziom spójności programu bezpieczeństwa wewnętrznego, a także rzeczywiste czynniki warunkujące zgodność audytu. Jeśli luki w zabezpieczeniach systemu i ryzyko biznesowe będą stale narastać między zaplanowanymi audytami zewnętrznymi, kierownictwo będzie musiało zbadać pierwotną przyczynę tego niestabilnego, cyklicznego zachowania. Chargeback odnosi się do możliwości pobierania opłat za korzystanie z usług IT. Niektóre organizacje uwzględniają te koszty w ogólnych kosztach prowadzenia działalności, zamiast rozliczać osoby i działy. Niezależnie od preferencji finansowych, włączenie monitorowania obciążenia zwrotnego w środowisku zapewnia zrozumienie, w jaki sposób wykorzystywane są zasoby informacyjne. Jeśli wykorzystanie działu marketingu wzrosło z 40 do 70 procent przepustowości łącza internetowego, a wykorzystanie pomocy technicznej wzrosło z 30 do 50 procent zasobów przetwarzania w chmurze, trendy mogą zachęcić kierownictwo do dostosowania zasobów w celu zaspokojenia popytu biznesowego lub zbadania nadużyć zasobów . Monitorowanie wykorzystania zasobów i zapotrzebowania na nie może również przynieść korzyści cyklom opracowywania i testowania, dzięki czemu zasoby produkcyjne są odpowiednio alokowane. Systemy obciążeń zwrotnych, takie jak wewnętrzne usługi rozliczeniowe i te używane przez zewnętrzne biura usług, okazują się cenne w monitorowaniu i śledzeniu działań systemu za pomocą ich dzienników. W niektórych stanach i miastach przepisy wymagają, aby tego typu usługi prowadziły dokładne dzienniki do celów kontrolnych. Oryginalne zapisy służą nie tylko do śledzenia, ale także w sprawach sądowych jako dowód. W większości sytuacji zarówno usługi wewnętrzne, jak i zewnętrzne są drugorzędnym „dowodem" transakcji, podczas gdy pierwotnym dowodem są początkowe logi systemowe. Zapisy plików dziennika stanowią podstawę zaawansowanych algorytmów rozliczeniowych, które zachęcają do racjonalnego wykorzystania zasobów. Ponadto, ponieważ nieoczekiwane zmiany w wydatkach mogą wzbudzić zainteresowanie personelu księgowego i menedżerów, systemy rozliczeniowe mogą czasami pomóc w identyfikacji nieautoryzowanego użycia na podstawie wzorców historycznych. Raporty o wyjątkach koncentrują się na określonych anomaliach danych, takich jak raporty o wydatkach pracowniczych, które nagle przekraczają 9 000 USD. Menedżerowie mogą chcieć zastosować ciągłe monitorowanie systemu finansowego w celu oceny trendów zgłoszeń wyjątków. Oprócz nadużyć i oszustw raporty o wyjątkach mogą identyfikować problemy systemowe. Generowanie raportów o wyjątkach dla systemów, które regularnie działają poniżej akceptowalnego poziomu wydajności, może wskazywać na awarię komponentu. Kierownictwo w zakładzie przemysłowym, który regularnie nie uwzględnia brakujących produktów, może odkryć problemy proceduralne, które skutkują zmarnowaniem materiału lub wadliwym sprzętem, który musi zostać naprawiony, aby rozwiązać problem trwającej utraty produktu. Raporty o wyjątkach mogą również identyfikować pojedynczy problem lub powszechny problem. Gdyby zarządzanie zmianami zarejestrowało wymianę sprzętu w pięciu segmentach potoku i wszystkie zaczęły przeciekać w tym samym czasie, zagregowane dane dziennika i raporty o wyjątkach wspierałyby potrzebę przeglądu

sprzętu i procedur. Lub raport wyjątku, oparty na danych z czujników zebranych w listopadzie 2002 wzdłuż uskoku Denali,18 może korelować z problemem środowiskowym (np. trzęsieniem ziemi), który prawdopodobnie wyjaśniałby przyczynę nieprawidłowego działania sprzętu.

Pulpity nawigacyjne

Pulpity nawigacyjne konsolidują informacje w odpowiednie i łatwe do zrozumienia podsumowanie. W zależności od potrzeb zarządzania i możliwości systemu można zastosować elementy tekstowe, wizualne i dźwiękowe. Pulpity nawigacyjne opierają się na technologii internetowej z zapleczem bazy danych, aby prezentować ogólny przegląd stanu operacyjnego z częstotliwością odświeżania zbliżoną do rzeczywistej. Wykresy, wykresy, wskaźniki sygnalizacji świetlnej (czerwony, żółty, zielony), wizualizacje systemowe i banery ostrzegawcze poprawiają komfort korzystania z pulpitu nawigacyjnego, jeśli są używane z umiarem. Pracownicy zazwyczaj przeglądają pulpity nawigacyjne za pomocą standardowej przeglądarki internetowej lub dużych ekranów wideo zamontowanych w centrach dowodzenia i obszarach wspólnych. Przy wdrażaniu specjalistycznych systemów M&C należy również wziąć pod uwagę pulpity nawigacyjne dla poszczególnych działów i kierownictwa. W zależności od wrażliwości informacji, obracanie pulpitów nawigacyjnych na wspólnych ekranach lub w samym portalu internetowym może być okazją do zwiększenia świadomości pracowników w zakresie wyników całej organizacji i poszczególnych działów. Współpracownicy mogą dowiedzieć się więcej o aktualnym poziomie ryzyka biznesowego, bieżącej wydajności operacyjnej (np. czasie pracy systemu, generowanych produktach lub wielkości sprzedaży), a nawet o aktualnym stanie cyberbezpieczeństwa. Oprócz pulpitów nawigacyjnych organizacje nadal używają wielu konsol zarządzania systemem do monitorowania i kontrolowania określonych elementów w infrastrukturze. Konsole do zarządzania systemem często są bardziej przeznaczone dla personelu technicznego niż dla wyższego kierownictwa. Konsole zarządzania systemem i pulpity nawigacyjne prawdopodobnie będą nadal współistnieć ze względu na potrzeby funkcjonalne.

Ochrona konfiguracji

Kiedy wdrażane są nowe systemy lub starsze systemy są dostosowywane do określonych poziomów zgodności, pojawiają się problemy z konfiguracją. Chociaż standardy oparte na zasadach mogą poprawnie definiować odpowiednie konfiguracje w celu ochrony zasobów informacyjnych, brak konsekwentnego stosowania szablonów konfiguracji lub list kontrolnych wprowadza niepotrzebną złożoność do zarządzania lukami w zabezpieczeniach i konfiguracją. Aby sprostać temu wyzwaniu, systemy M&C mogą identyfikować anomalie i przywracać zgodność systemów przy użyciu wstępnie zdefiniowanych kryteriów. Standard Payment Card Industry Data Security Standard (PCI DSS) wymaga wykrywania integralności plików i ostrzegania. Jednak organizacja może również uznać za korzystne wdrożenie systemu, który będzie automatycznie wykrywał, ostrzegał i korygował rozbieżności w integralności systemu podczas raportowania niezgodnych plików lub ustawień. W przemysłowych systemach sterowania (ICS) programowalne sterowniki logiczne (PLC) przechowują i uruchamiają programy logiki drabinkowej do sterowania urządzeniami sprzętowymi w terenie. Programiści lub automatycy aktualizują te programy za pomocą specjalistycznego oprogramowania dla sieci przemysłowych. Modyfikacja programu wpłynie bezpośrednio na wyjście siłowników podłączonych do PLC. Na przykład nieprawidłowa modyfikacja nastawy czujnika zbiornika na wartość większą niż pojemność zbiornika może spowodować utratę produktu, co wymaga ręcznego ustawienia. Z tego powodu program musi być chroniony przed złośliwymi i przypadkowymi zmianami. Używanie hasła do ochrony uruchomionego programu i warstwowych zabezpieczeń sieciowych, takich jak sieciowy IPS, przyczynia się do ochrony konfiguracji w tym scenariuszu.

Rozważania dotyczące wydajności

Podobnie jak wszystkie systemy, systemy M&C wymagają zasobów do działania. W zależności od modelu operacyjnego zasoby te mogą pochodzić z tego samego systemu hosta, połączenia sieciowego lub urządzenia zdalnego. Niezmierzenie wpływu systemu monitorowania na wydajność może doprowadzić do pogorszenia stanu środowiska operacyjnego. Ponadto wdrażanie nowych systemów podczas dużego obciążenia w cyklu biznesowym może zakłócić normalną działalność. Zainstalowanie korporacyjnego systemu monitorowania integralności plików i wykonanie analizy bazowej systemów produkcyjnych w godzinach szczytu może doprowadzić do nadmiernego wykorzystania zasobów systemowych i wstrzymania krytycznych zadań produkcyjnych. Zmiany w M&C wymagają planowania i koordynacji z odpowiednimi jednostkami biznesowymi i personelem technicznym, aby zapewnić, że nowe systemy spełniają zarówno potrzeby biznesowe, jak i wymagania techniczne, aby działać wydajnie.

WYZWANIA DOTYCZĄCE MONITOROWANIA I KONTROLI

Starsze systemy nie zawsze posiadają wystarczającą M&C dla dzisiejszych wymagań biznesowych i regulacyjnych. Sztuka modernizacji zabezpieczeń w istniejącym systemie wymaga pokonania barier fizycznych, technicznych i psychospołecznych. Bariery fizyczne obejmują zarówno przewodowe instalacje ICS, jak i bezprzewodową komunikację mobilną. Kwestie techniczne obejmują naukę wykrywania i monitorowania unikalnych protokołów komunikacyjnych, zrozumienie wymagań dotyczących wydajności produkcji oraz zarządzanie

SYSTEMY MONITOROWANIA I KONTROLI

Wyzwania psychospołeczne są często najtrudniejsze. Organizacje i sektory biznesowe, które nie są przyzwyczajone do dojrzałych systemów M&C, zazwyczaj zaprzeczają, że takie systemy są potrzebne. Próby racjonalizacji zwykle obejmują zaprzeczenie, że atakujący kiedykolwiek zaatakuje ich systemy, twierdzenie, że firma działa dobrze, oraz obawy, że dodatkowe zmiany lub złożoność prawdopodobnie zakłócą produkcję. Szkolenie w zakresie świadomości bezpieczeństwa i zmiany w przywództwie mogą częściowo rozwiać te błędne przekonania, jednocześnie wskazując na brak dostępnych danych M&C na poparcie wszelkich twierdzeń, że operacje działają tak wydajnie i bezpiecznie, jak powinny.

Przemysłowe systemy sterowania

Przemysłowe systemy sterowania (ICS) działają w wielu gałęziach przemysłu, w tym w przemyśle naftowym, wodnym i energetycznym. Systemy ICS są ogólnie podzielone na rozproszone systemy sterowania (DCS) oraz systemy kontroli nadzorczej i akwizycji danych (SCADA). DCS są częściej kojarzone z procesami takimi jak rafinacja ropy naftowej. Systemy SCADA wymagają większej interakcji człowieka za pośrednictwem HMI i zbierają dane z wielu zdalnych urządzeń. Niektóre systemy zawierają elementy zarówno DCS, jak i SCADA. Problemy z bezpieczeństwem wzrosły ze względu na łączność sieciową i zagrożenia dla infrastruktury krytycznej. Oczekuje się, że systemy te będą nadal integrować się w skali globalnej, z ulepszoną, scentralizowaną agregacją danych i raportowaniem. Kierownictwo znajdzie wartość nie tylko w agregowaniu danych własnej organizacji, ale także we współpracy na forach branżowych w celu wdrożenia bardziej stabilnych, interoperacyjnych i bezpiecznych przemysłowych systemów M&C. Podobnie jak komputery typu mainframe, systemy SCADA nie działają już w odizolowanym środowisku. Lokalizacje często komunikują się za pośrednictwem łączy dzierżawionych, satelity i modemów telefonicznych. Niektóre zakłady przemysłowe wykorzystują sprzęt bezprzewodowy ZigBee zamiast instalować standardowe okablowanie do monitorowania i sterowania urządzeniami zdalnymi. Technicy łączą się przez modem lub tunel wirtualnej sieci prywatnej (VPN) przez Internet, aby zdalnie zarządzać systemami przemysłowymi. Inne bezpośrednie połączenia z Internetu (przez Pulpit zdalny lub VNC) mogą również istnieć, ale nie są zalecane. Wyzwania M&C dla tych systemów obejmują uwierzytelnianie,

bezpieczeństwo sieci, ochronę konfiguracji i bezpieczeństwo fizyczne. W przeszłości uwierzytelnianie nie było wymagane, aby używać komputera PC do bezpośredniej komunikacji ze sterownikiem PLC przez sieć SCADA. Niektórzy dostawcy próbują teraz wbudować uwierzytelnianie w interfejs HMI. Jednak protokoły sieciowe używane w systemie SCADA (np. MODBUS/TCP, DNP3) mogą nadal wysyłać do PLC niezamówione komunikaty w celu wykonania dowolnych poleceń. Ochrona konfiguracji jest typowa związana z uruchomionym programem na sterowniku PLC, który może mieć słabe lub nieistniejące hasło. Z punktu widzenia operatora, HMI zwykle działa na niezałatanym komputerze z kontrolą bezpieczeństwa na poziomie aplikacji. Kontrole te są zwykle omijane przez atakowanie niewłaściwie zabezpieczonego systemu operacyjnego lub włożenie zainfekowanego dysku USB. Laptopy używane przez inżynierów do zarządzania i aktualizowania programów PLC wykraczają poza dotychczasowe granice szczeliny powietrznej i często są podłączone do niezaufanych sieci zewnętrznych, używane do obsługi Internetu i poczty e-mail oraz narażone na fizyczne ataki poza siedzibą firmy. Bezpieczeństwo fizyczne pozostaje wyzwaniem, ponieważ sprzęt może nie znajdować się w zabezpieczonym obszarze lub operatorzy mogą nie mieć odpowiedniego szkolenia w zakresie świadomości bezpieczeństwa, aby wdrożyć odpowiednie procedury bezpieczeństwa. Na szczęście te systemy M&C mogą wykorzystywać istniejące zasoby bezpieczeństwa informacji do ograniczania ryzyka w architekturze warstwowej. NIST SPEC PUB 800-82 jasno opisuje krajobraz bezpieczeństwa otaczający te systemy. Zapory sieciowe, systemy zapobiegania włamaniom i solidniejsze zabezpieczenia fizyczne przyczyniłyby się do zwiększenia bezpieczeństwa środowiska SCADA. Narzędzia do wykrywania luk w zabezpieczeniach integrują teraz protokoły SCADA w celu wykrywania luk w zabezpieczeniach i ograniczania ryzyka. Dalsze opracowywanie bezpieczniejszych protokołów komunikacyjnych i ustanawianie wytycznych dotyczących ochrony konfiguracji jeszcze bardziej poprawiłoby słabe punkty uwierzytelniania we wdrożeniach SCADA. M&C w środowisku ICS stają się bardziej złożone ze względu na własność i obowiązki. Tradycyjne organizacje IT często obsługują sieci aż do portu sieciowego, ale często brakuje im specjalistycznej wiedzy i specjalistycznej wiedzy na temat przemysłowych środowisk sterowania. Inżynierowie automatycy mogą wdrażać określone elementy sieci w oparciu o wymagania produkcyjne, bez konieczności dostosowywania konfiguracji do wymagań bezpieczeństwa i polityki

Komputery mobilne

Ponieważ nadal integrujemy mobilne i rozproszone systemy obliczeniowe, rośnie złożoność i trudność wymagane do zabezpieczenia systemów. Mamy więcej zmiennych do rozwiązania. Informacje płyną jeszcze dalej od tradycyjnego obwodu sieci. Organizacje nadal wspierają zasady przynoszenia własnego urządzenia (BYOD), które wprowadzają do środowiska niezaufane i niezabezpieczone węzły sieciowe; te urządzenia osobiste przechowujące dane firmowe powinny być objęte bardzo jasno określonymi zasadami i standardami. Dzięki postępom w deperymetryzacji systemy M&C muszą zapewniać bezpieczeństwo danych podczas ich przesyłania i spoczynku, zgodnie z zasadami organizacji. Technologie mobilne komunikują się za pośrednictwem łączy bezprzewodowych, niewidocznych dla tradycyjnych systemów M&C. Niektóre urządzenia bezprzewodowe wymagają scentralizowanego zarządzania systemem, ale rzadko łączą się z siecią korporacyjną. Szyfrowanie mobilne i obowiązkowa łączność VPN pomagają kontrolować przechowywanie i transmisję danych. Dzięki scentralizowanym zasadom systemy te promują bardziej spójną komunikację danych w całej organizacji. Systemy monitorowania z wykorzystaniem identyfikacji radiowej (RFID) bezprzewodowo identyfikują i zbierają informacje z systemu docelowego. NIST 800-98 opisuje technologiczne korzyści i zagrożenia związane z wdrożeniem tej technologii. Systemy M&C często zbierają poufne informacje. Kwestie prywatności związane z RFID będą wymagały dokładnej oceny ryzyka, aby uniknąć potencjalnej utraty danych. Oznaczanie wszystkich pracowników organizacji identyfikatorami RFID, które zawierają dane osobowe podlegające przepisom HIPAA, byłoby nierozsądne, ponieważ do tagów RFID można potencjalnie

uzyskać dostęp z odległości większej niż jeden metr bez wiedzy posiadacza. Z punktu widzenia inwentaryzacji tagi RFID umożliwiają automatyzację audytów zasobów firmy lub gromadzenie informacji o aktywach bez konieczności ich ręcznego zapisywania. Aby uniknąć kompromisu, standardy urządzeń wykorzystują kontrole integralności (CRC) i wymagają hasła, aby uniemożliwić im reagowanie.

Wirtualizacja

Organizacje używają różnych urządzeń komputerowych, aby zaspokoić swoje potrzeby biznesowe. Niektóre urządzenia mogą nie być w pełni wykorzystywane, a krytyczne serwery baz danych wymagają dodatkowej przestrzeni dyskowej i pamięci roboczej. Wirtualizacja zapewnia możliwość dzielenia i łączenia zasobów obliczeniowych w bardziej wydajne, ukierunkowane i często przenośne zasoby biznesowe. Systemy wirtualne zazwyczaj składają się ze sprzętu fizycznego, interfejsu wirtualizacji (VI) i maszyny wirtualnej (VM). Maszyna wirtualna może być aplikacją lub całym systemem operacyjnym. Ponieważ VI nadzoruje maszyny wirtualne, musimy wdrożyć odpowiednie M&C w warstwie VI, jak również w obrębie i wokół maszyn wirtualnych. Użytkownicy zwirtualizowanego systemu operacyjnego mogą nie być w stanie wykryć, że jest on zwirtualizowany. Na przykład firma hostingowa może chcieć udostępnić swoim klientom dedykowane serwery wirtualne bez dodatkowych wydatków na dedykowany sprzęt. W tej sytuacji organizacja może wdrożyć serwery FreeBSD i wdrożyć pewien stopień wirtualizacji przy użyciu „więzień”21, aby zapewnić klientom wysoki poziom podzielonego na sekcje dostępu na poziomie systemu. Operator z uprawnieniami administratora do uwięzionego środowiska nie powinien widzieć procesów wykonywanych przez inne więzienia ani podstawowy system obsługujący więzienia. Jednak właściciel systemu hosta może monitorować lub kontrolować elementy systemu hosta, jak również te w środowiskach uwięzionych. Może być również konieczne dodatkowe monitorowanie systemu hosta w celu wykrycia prób jailbreak. Inny rodzaj wirtualizacji, parawirtualizacja, wykorzystuje hiperwizora jako VI między sprzętem a maszyną wirtualną. Zamiast tworzyć identyczne środowiska uwięzione, hiperwizor może być używany do obsługi więcej niż jednego typu gościnnej maszyny wirtualnej, takiej jak Ubuntu, Fedora i PC-BSD. Ta konfiguracja jest możliwa, ponieważ hiperwizor obsługuje całą komunikację (hiperpołączenia) między sprzętem a maszynami wirtualnymi. Na tej samej zasadzie, co host FreeBSD z więzieniami, hiperwizor może monitorować i kontrolować działania w maszynach wirtualnych i wokół nich z różnym stopniem przejrzystości dla użytkownika maszyny wirtualnej. Możliwość monitorowania maszyn wirtualnych w trybie stealth sprawia, że wirtualizacja jest użytecznym narzędziem monitorowania do badań pułapek typu honeypot. Aby uzyskać wyższy poziom bezpieczeństwa systemu, organizacje będą potrzebowały narzędzi do wykrywania i zapobiegania atakom na hiperwizora. Przenośność, zaleta wirtualizacji, stanowi wyzwanie dla systemów M&C. Maszyny wirtualne mogą często migrować z jednego urządzenia sprzętowego na inne, podczas gdy integralność maszyny wirtualnej offline jest nieznana. W zarządzanej, zwirtualizowanej infrastrukturze problemy z wydajnością wykryte w VI mogą spowodować migrację maszyn wirtualnych z jednego serwera fizycznego do mniej wykorzystywanego zasobu. Niestabilna maszyna wirtualna może również zostać ręcznie wyłączona z sieci i szybko ponownie wdrożona przy użyciu zapasowego dysku wirtualnego, bez zakłócania pracy innych maszyn wirtualnych korzystających z tego samego sprzętu fizycznego. Śledzenie tych ruchomych celów wymaga niezawodnego dostępu do wirtualnej puli zasobów, dokumentacji mapowania zasobów wirtualnych na fizyczne, a także jasno określonej polityki udostępniania systemu wirtualnego. Na przykład organizacja, której zasady wymagają wyraźnego oddzielenia systemów poufnych od publicznych, powinna zabronić tym samym hiperwizorom zarządzania zarówno aplikacjami płacowymi, jak i publicznymi maszynami wirtualnymi kiosku na tych samych hostach.

Chmura obliczeniowa

Przetwarzanie w chmurze wykorzystuje kilka modeli wdrażania i usług w celu zapewnienia elastycznych zasobów obliczeniowych i pamięci masowej. M&C w chmurze wiąże się jednak z dodatkowymi wyzwaniami ze względu na różnice we wdrożeniach i dodatkowe strony zaangażowane w zadania funkcjonalne. W chmurach publicznych odpowiedzialność za środowisko fizyczne i infrastrukturę sieciową M&C spoczywa na dostawcy usług hostingowych. W rezultacie organizacje mają znacznie mniejszy wgląd w codzienne operacje sieciowe i działania związane z obsługą incydentów i muszą polegać na zaświadczeniach stron trzecich i standardowych raportach (np. SAS 70, SSAE 16). Zmniejszona widoczność M&C zwiększa zależność od umów między dostawcą chmury a dzierżawcą chmury. Wytyczne opublikowane przez ENISA i Cloud Security Alliance mogą pomóc w analizie kosztów i korzyści związanych z ryzykiem. Oprócz standardowych potrzeb w zakresie zasobów obliczeniowych i pamięci masowej, organizacje mogą również wykorzystywać zasoby chmury do zarządzania dziennikami, odtwarzania po awarii i izolacji środowiska programistycznego. Odpowiedzialność za bezpieczeństwo i możliwości M&C są większe w przypadku organizacji korzystającej z modelu infrastruktury jako usługi (Iaas) niż w przypadku innych modeli usług. Instancje systemu wirtualnego można skonfigurować ze standardowymi możliwościami rejestrowania na poziomie systemu operacyjnego i aplikacji. Jednak niektóre elementy sprzętowe, takie jak pamięć, mogą być współdzielone z sąsiednimi dzierżawcami chmury. Platforma (PaaS) i oprogramowanie jako usługa (SaaS) zapewniają klientom mniejszą widoczność poza środowiskiem aplikacji. Zarządzanie zasobami w chmurze może odbywać się za pośrednictwem standardowego interfejsu WWW i interfejsów API. Chociaż wiele elementów monitorowania i kontroli może nadal istnieć, podejście do uzyskiwania dostępu do danych i ich przechowywania może się różnić. Na przykład administrator może utworzyć migawkę działającej instancji bez wpływu na system produkcyjny. Ponadto migawka może zostać zamontowana w chmurze w celu przeprowadzenia działań następczych. Kontrolowanie dostępu do kluczy, interfejsów zarządzania, maszyn wirtualnych i woluminów pamięci masowej to ważne cele dla M&C w chmurze. Ponadto, jeśli to możliwe, należy również rozważyć szyfrowanie danych.

STRESZCZENIE

Systemy monitorowania i kontroli zapewniają zainteresowanym stronom technologicznym dodatkową pewność związaną z działaniem systemu. M&C umożliwiają wgląd w operacje produkcyjne, a także mogą wykrywać i zapobiegać niepożądanym zdarzeniom i nieefektywności operacyjnej. Kontrolowanie każdego elementu systemu informatycznego jest generalnie niepraktyczne z punktu widzenia kosztów i ryzyka. Jednak przyjmując podejście oparte na ryzyku, możemy określić, co powinno być monitorowane, kontrolowane lub akceptowane jako ryzyko rezydualne. Przepisy, zasady wewnętrzne, ramy branżowe, wymagania biznesowe i potrzeby operacyjne mają wpływ na proces decyzyjny przy wyborze i wdrażaniu systemów i funkcji M&C. Zdefiniowany zakres i wymagania biznesowe decydują o wyborze odpowiedniego modelu M&C. Podczas gdy interakcja człowieka nadal odgrywa kluczową rolę w starszych systemach, zwiększone wyrafinowanie automatyzacji może prowadzić do lepszych możliwości raportowania i ciągłej pewności. Wyjątkowe wyzwania związane z powierzchnią automatyki w środowiskach o specyficznych wymaganiach, w tym kontroli przemysłowych. Monitorowanie, kontrola i audyty przesłuchują systemy informacyjne, identyfikują problemy, inicjują działania naprawcze i generują znaczące informacje o stanie różnych systemów i procesów. Systemy mogą obejmować interakcję człowieka lub działać w zautomatyzowanym, zamkniętym formacie. Systemy generują pliki dziennika na podstawie działań systemowych, przechowują je w bezpiecznych lokalizacjach i umożliwiają agregatorom gromadzenie danych i przekształcanie ich w przydatne informacje. Chociaż agregacja dzienników usprawnia proces analizy, zasoby wymagane do przechowywania danych i manipulowania nimi mogą stać się problematyczne. Nie wszystkie wydarzenia są przydatne. Aby zarządzać rozsądnymi ilościami danych, centralny system zarządzania powinien rejestrować lub gromadzić tylko określone działania. Dane z pliku dziennika umożliwiają

historyczną analizę zdarzeń w dowolnym zmierzonym momencie — niezbędny element zarządzania infrastrukturą. Organizacje muszą zrozumieć wartość aktywów, dostosować działalność biznesową do wymogów prawnych i znaleźć nowe sposoby wykorzystania M&C w celu poprawy wydajności operacyjnej.