NOWE RAMY BEZPIECZEŃSTWA INFORMACJI

PROPOZYCJE DOTYCZĄCE NWEGO SYSTEMU BEZPIECZEŃSTWA

Bezpieczeństwo informacji historycznie zostało ograniczone przez brak kompleksowych, kompletnych i analitycznie zdrowych ram dla analizy i doskonalenia. Trwałość klasycznej triady CIA (poufność, integralność, dostępność) jest niewystarczająca, aby opisać to, co praktycy bezpieczeństwa uwzględniają i wdrażają podczas wykonywania swojej pracy. Potrzebujemy nowej struktury bezpieczeństwa informacji, która będzie kompletna, poprawna i spójna w celu wyrażenia, w języku praktycznym, środków dla właścicieli informacji w celu ochrony ich informacji przed wszelkimi przeciwnościami i słabymi punktami. Obecny nacisk na bezpieczeństwo systemów komputerowych można przypisać zrozumiałej tendencji informatyków do ochrony tego, co wiedzą najlepiej - systemów komputerowych i sieciowych, a nie stosowania tych systemów. Z technologicznym młotkiem w dłoni wszystko wygląda jak gwóźdź. Podstawowe wyzwanie bezpieczeństwa pojawia się od osób nadużywających lub nadużywających informacji, a często - ale niekoniecznie - za pomocą komputerów i sieci. Jednak osoby, które obecnie dominują nad informacjami bezpieczeństwa sztuki ludowej nie są ani kryminologami, ani specjalistami od aplikacji komputerowych. Przedstawimy kompleksowe nowe ramy bezpieczeństwa informacji, które rozwiązują problemy istniejących modeli. Demonstrujemy potrzebę sześciu elementów bezpieczeństwa - dostępność, użyteczność, integralność, autentyczność, poufność i posiadanie - w celu zastąpienia niekompletnego bezpieczeństwa CIA (które nawet nie wydaje się zawierać zabezpieczeń dla informacji, które nie są poufne) w nowych ramach bezpieczeństwa. Ta nowa struktura służy do wyliczenia wszystkich aspektów bezpieczeństwa na poziomie podstawowym. Ramy są również przedstawiane w innej formie: Zagrożenia, zasoby, model podatności, który zawiera szczegółowe deskryptory dla każdego tematu w modelu. Model ten wspiera nowe ramy bezpieczeństwa, demonstrując swój wkład w zwiększanie bezpieczeństwa informacji od jego obecnego etapu technologicznego oraz jako sztuki ludowej, w podstawy inżynierii i sztuki biznesowej w cyberprzestrzeni. Nowy model ramowy bezpieczeństwa obejmuje sześć istotnych części:

1. Elementami bezpieczeństwa informacji, które należy chronić są:

* Dostępność

* Użyteczność

* Integralność

* Autentyczność

* Poufność

* Posiadanie

2. Źródła utraty tych elementów informacji bezpieczeństwa:

* Zwolennicy i niewłaściwi użytkownicy

* Przypadkowe zdarzenia

* Naturalne siły fizyczne

3. Akty powodujące utratę:

* Zniszczenie

* Zakłócenia w użyciu

* Używanie fałszywych danych

* Modyfikacja lub wymiana

* Błędne przedstawienie lub odrzucenie

* Niewłaściwe użycie lub niewykorzystanie

* Lokalizacja

* Ujawnienie

* Obserwacja

* Biurowe

* Nabierające

* Zagrożenie

4. Funkcje ochronne w celu ochrony informacji przed tymi działaniami:

* Rewizja

* Unikanie

* Odstraszenie

* Wykrycie

* Zapobieganie

* Łagodzenie

* Przenoszenie

* Dochodzenie

* Sankcje i nagrody

* Poprawa

5. Metody selekcji zabezpieczeń:

* Wykorzystaj należytą staranność

* Przestrzegaj przepisów i norm

* Włącz firmę

* Spełniaj specjalne potrzeby

6. Cele do osiągnięcia dzięki bezpieczeństwu informacji:

* Unikaj zaniedbania

* Spełniać wymagania przepisów i regulacji

* Zaangażuj się w udany handel

* Zaangażuj się w etyczne postępowanie

* Chroń prywatność

* Minimalizuj wpływ bezpieczeństwa na wydajność

* Wspieraj uporządkowane i chronione społeczeństwo

Podsumowując, model ten opiera się na dążeniu do zaspokojenia potrzeb właścicieli w zakresie ochrony pożądanych elementów bezpieczeństwa ich informacji przed źródłami strat, które angażują się w szkodliwe działania i zdarzenia poprzez stosowanie funkcji zabezpieczających, które są wybierane za pomocą zaakceptowanych metod w celu osiągnięcia pożądanych celów. Sekcje modelu zostały wyjaśnione poniżej. Należy zauważyć, że ryzyko bezpieczeństwa, zwrot z inwestycji w bezpieczeństwo (ROSI) i wartość bieżąca netto (NPV) w oparciu o nieznane przyszłe straty i wrogów oraz ich intencje nie zostały zidentyfikowane w tym modelu, ponieważ nie są one mierzalne, a zatem nie do opanowania

SZEŚĆ PODSTAWOWYCH ELEMENTÓW BEZPIECZEŃSTWA

Sześć elementów bezpieczeństwa w proponowanym modelu ramowym ma zasadnicze znaczenie dla bezpieczeństwa informacji. Jeśli którykolwiek z nich zostanie pominięty, bezpieczeństwo informacji jest niewystarczające w ochronie właścicieli informacji. Sześć scenariuszy utraty informacji, wszystkie oparte na rzeczywistych przypadkach, wykorzystuje się do wykazania tego sporu. Pokazujemy, jak każdy scenariusz wiąże się z naruszeniem jednego i tylko jednego elementu bezpieczeństwa informacji. Dlatego jeśli pominiemy ten element z bezpieczeństwa informacji, usuniemy ten scenariusz z obaw związanych z bezpieczeństwem informacji, co byłoby nie do przyjęcia. Jest prawdopodobne, że specjaliści ds. Bezpieczeństwa informacji zgodzą się, że wszystkie te scenariusze mieszczą się w zakresie nadużyć i nadużyć, których musimy chronić.

Scenariusz straty 1: Dostępność

Odrzucony programista kontraktowy, zamierzający sabotować, usunął nazwę pliku danych z katalogów plików w komputerze unii kredytowych. Użytkownicy komputera i pliku danych już nie mieli do niego dostępu, ponieważ system operacyjny komputera rozpoznaje istnienie informacji dostępnych dla użytkowników tylko wtedy, gdy są one nazwane w katalogach plików. Unia kredytowa została zamknięta na dwa tygodnie, podczas gdy inny programista został sprowadzony, aby znaleźć i rozwiązać problem, aby plik był dostępny. Sprawca został w końcu skazany za przestępstwa komputerowe. Z wyjątkiem dostępności, pozostałe elementy bezpieczeństwa informacji - użyteczności, integralności, autentyczności, poufności i posiadania - nie rozwiązują tej straty, a ich stan nie zmienia się w scenariuszu. Właściciel komputera (unia kredytowa) zachował własność pliku danych. Tylko dostępność informacji została utracona, ale jest to strata, której wyraźnie powinno zapobiegać bezpieczeństwo informacji. W związku z tym zachowanie dostępności musi być akceptowane jako cel bezpieczeństwa informacji. Prawdą jest, że dobra praktyka w zakresie bezpieczeństwa mogła zapobiec niezadowoleniu programisty z używania systemu aplikacji unii kredytowych, a kierownictwo kasy mogło bardziej uważnie monitorować swoją pracę. Nie powinny one być zależne od technicznych możliwości i wiedzy tylko jednej osoby i powinno było ono używać kilku mechanizmów kontrolnych do zachowania lub przywracania dostępności plików danych w komputerze, na przykład przez utrzymywanie katalogu kopii zapasowych z nazwami usuniętych plików i wskaźniki do ich fizycznej lokalizacji. Utracie można było zapobiec lub zminimalizować dzięki dobrym procedurom tworzenia kopii zapasowych, dobrym kontrolom użytkowania komputerów i określonych plików danych, wykorzystaniu więcej niż jednej nazwy do zidentyfikowania i znalezienia pliku oraz dostępności programów narzędziowych do wyszukiwania plików według zawartości lub do przechowywania plików lustrzanych. Zabezpieczenia te przynajmniej utrudniłyby atak i zmusiły programistę do popełnienia nadużycia w jego działaniu. Nasilenie utraty dostępności może się znacznie różnić. Sprawca może

zniszczyć kopie pliku danych w sposób, który eliminuje jakiekolwiek szanse na odzyskanie. W innych sytuacjach plik danych może być częściowo użyteczny, a odzyskiwanie możliwe za umiarkowany koszt, lub użytkownik może mieć niedogodności lub opóźnienia w korzystaniu z pliku przez pewien okres czasu, a następnie pełne odzyskanie.

Scenariusz straty 2: Użyteczność

W takim przypadku pracownik rutynowo zaszyfrował jedyną kopię cennych informacji przechowywanych w komputerze swojej organizacji, a następnie przypadkowo skasował klucz szyfrowania. Przydatność informacji została utracona i można ją było przywrócić jedynie poprzez trudną kryptoanalizę. Chociaż ten scenariusz można opisać jako utratę dostępności lub autentyczności klucza szyfrowania, utrata skupia się na użyteczności informacji, a nie na kluczu, ponieważ jedynym celem tego klucza było ułatwienie szyfrowania. Informacje w tym scenariuszu są dostępne, ale w formie, która nie jest przydatna. Jego integralność, autentyczność i posiadanie pozostają nienaruszone, a ich poufność została niestety znacznie poprawiona. Aby zachować użyteczność informacji w tym przypadku, zarządzanie powinno wymagać obowiązkowych kopii zapasowych wszystkich krytycznych informacji i powinno kontrolować użycie potężnych mechanizmów ochronnych, takich jak kryptografia. Kierownictwo powinno wymagać przeprowadzenia testów zabezpieczeń podczas tworzenia aplikacji, aby ograniczyć nieużyteczne formy informacji. Powinno to zminimalizować niekorzystny wpływ bezpieczeństwa na wykorzystanie informacji i powinno kontrolować rodzaje działań, które umożliwiają nieupoważnionym osobom zmniejszenie przydatności informacji. Utrata użyteczności może mieć różny stopień ważności. Najgorszym scenariuszem byłaby całkowita utrata przydatności informacji, bez możliwości odzyskania. Mniej poważne przypadki mogą obejmować stan częściowo przydatny z możliwością pełnego przywrócenia przydatność przy umiarkowanych kosztach.

Scenariusz straty 3: Integralność

W tym scenariuszu dystrybutor oprogramowania kupił kopię (na DVD) programu do gry komputerowej od nieznanego wydawcy. Dystrybutor wykonał kopie DVD i usunął nazwisko wydawcy z kopii DVD. Następnie, bez informowania wydawcy lub płacenia tantiem, dystrybutor sprzedał kopie DVD w obcym kraju. Niestety, sukcesu sprzedaży programu nie powstrzymał brak zidentyfikowanego wydawcy na DVD lub w materiałach promocyjnych produktu. Ponieważ kopie DVD gry nie identyfikują wydawcy, który utworzył program, kopie nie były spójne. ("Integralność" oznacza stan kompletności, całości i poprawności lub przestrzeganie kodeksu wartości moralnych.) Jednak kopie nie były pozbawione autentyczności, ponieważ zawierały prawdziwy program gry i brakowało tylko tożsamości wydawcy, która nie była konieczna do pomyślnego użycia produktu. Narzędzie informacyjne DVD zostało zachowane, a poufność i dostępność nie były przedmiotem problemu. Posiadanie również nie było problemem, ponieważ dystrybutor kupił oryginalne DVD. Jednak w konsekwencji naruszono ochronę praw autorskich, utratę integralności i nieautoryzowane kopiowania autentycznego programu. Można zastosować kilka kontroli, aby zapobiec utracie integralności informacji, w tym używanie i sprawdzanie numerów porządkowych, sum kontrolnych i / lub sum kontrolnych w celu zapewnienia kompletności i całości dla szeregu elementów. Inne kontrole obejmują wykonywanie ręcznych i automatycznych sprawdzeń tekstowych pod kątem wymaganej obecności rekordów, podprogramów, akapitów lub tytułów oraz testowanie w celu wykrycia naruszeń określonych kontroli. Stopień utraty integralności informacji również jest różny. Istotne części informacji może być brakujący lub nieprawidłowy (ale wciąż dostępny), bez możliwości odzyskania. Lub brakujące lub nieuprawnione informacje można przywrócić z opóźnieniem i przy umiarkowanych kosztach. W najgorszych przypadkach właściciel może szybko odzyskać niewielkie ilości nieprawidłowo uporządkowanych lub zmonopolizowanych informacji po niskich kosztach

Scenariusz straty 4: Autentyczność

W odmianie poprzedniego scenariusza inny dystrybutor oprogramowania uzyskał program (na DVD) dla gry komputerowej od nieznanego wydawcy. Dystrybutor zmienił nazwę wydawcy na DVD i na ekranach tytułowych na nazwę znanego wydawcy, a następnie zrobił kopie płyty DVD. Bez poinformowania o tym wydawcy, dystrybutor następnie rozprowadzał kopie DVD w obcym kraju. W tym przypadku tożsamość popularnego wydawcy na płytach DVD iw materiałach promocyjnych znacznie przyczyniła się do sukcesu sprzedaży produktu. Ponieważ dystrybutor przeinaczył wydawcę gry, program nie był zgodny z rzeczywistością: nie był to autentyczna gra od znanego wydawcy. Dostępność i użyteczność nie są w tym przypadku kwestią sporną. Gra była uczciwa, ponieważ identyfikowała wydawcę i była kompletna i dobra. (Z pewnością dystrybutorowi brakowało osobistej uczciwości, ponieważ jego działania nie były zgodne z praktyką etyczną, ale nie jest to przedmiotem scenariusza.) Faktyczny wydawca nie stracił posiadania gry, mimo że kopie były oszukańczo reprezentowane jako pochodzące od innego wydawca. I chociaż dystrybutor niewątpliwie starał się zachować swoje działania w sekrecie przed oboma wydawcami, poufność treści gry nie była kwestią sporną. Co zrobić, jeśli ktoś błędnie przedstawi twoje informacje, twierdząc, że jest to jego? Naruszenie CIA nie obejmuje tego aktu. Makler giełdowy na Florydzie oszukał swoich inwestorów w schemacie Ponziego (piramida). Ukradł 50 milionów dolarów, twierdząc, że wykorzystał superszybki program komputerowy na swoim gigantycznym komputerze, aby osiągnąć zyski w wysokości 60 procent dziennie dzięki arbitrażowi, czyli metodzie handlu akcjami, w której inwestor wykorzystuje niewielką różnicę cen tego samego towaru w różnych rynki. Pokazał inwestorom komputer typu mainframe w firmie maklerskiej Wall Street i fałszywie twierdził, że to on i przechowywane w nim informacje były jego, tym samym użyczając wiarygodności swoim twierdzeniom o udanym handlu. Program maklera giełdowego był z pewnością przestępstwem komputerowym, ale elementy CIA nie odnoszą się do niego jako takiego, ponieważ jego definicja uczciwości nie obejmuje wprowadzania w błąd informacji. "Uczciwość" oznacza tylko, że informacje są pełne lub kompletne; nie odnosi się do ważności informacji. Oczywiście poufność i dostępność nie obejmują również wprowadzania w błąd. Najlepszym sposobem na rozszerzenie CIA o fałszywe przedstawienie jest użycie bardziej ogólnego określenia "autentyczność". Możemy wtedy przypisać prawidłowy zwrot "integralność informacji": całość, kompletność i dobry stan. Dr Peter Neumann z SRI International jest poprawny, gdy mówi, że informacje w sposób uczciwy oznaczają, że informacje są takie, jakich się spodziewasz. Nie oznacza to jednak, że informacje są ważne (możesz się spodziewać, że są one nieważne). "Autentyczność" to słowo oznaczające zgodność z rzeczywistością. W celu zapewnienia autentyczności informacji można zastosować wiele elementów sterujących. Obejmują one potwierdzanie transakcji, nazw, dostaw i adresów; zatwierdzanie produktów; sprawdzanie informacji spoza zakresu lub niepoprawnych; i używanie podpisów cyfrowych i znaków wodnych do uwierzytelniania dokumentów. Nasilenie utraty autentyczności może przybierać różne formy, w tym brak zgodności z rzeczywistością bez możliwości odzyskania; umiarkowanie fałszywe lub oszukańcze informacje z opóźnionym powrotem do zdrowia przy umiarkowanych kosztach; lub tylko poprawne informacje tylko denerwujące rozbieżności. Jeśli elementy CIA zawierały autentyczność, z fałszywym przedstawieniem informacji jako ważnego powiązanego zagrożenia, Kevin Mitnick (notoryczny haker kryminalny, który używał oszustwa jako swojego głównego narzędzia do penetrowania barier bezpieczeństwa) mógł stanąć przed znacznie trudniejszym wyzwaniem w popełnianiu zbrodni. Komputerowy przemysł mógł zrozumieć potrzebę udowodnienia, że aktualizacje systemu operacyjnego komputera i witryny sieci Web są autentyczne, aby uniknąć złych zamiarów

Scenariusz straty 5: Poufność

Złodziej oszukańczo uzyskał informacje od personelu technicznego banku. Użył skradzionego klucza, by otworzyć drzwi konserwacyjne bankomatu (ATM) i potajemnie włożył nadajnik radiowy, który kupił w sklepie Radio Shack. Radio otrzymywało sygnały z ekranu dotykowego w bankomacie używanym przez klientów do wprowadzania osobistych numerów identyfikacyjnych (PIN) i do otrzymywania informacji o saldzie konta. Urządzenie radiowe transmitowało informacje do odbiornika radiowego złodzieja w jego pobliskim samochodzie, który rejestrował kody PIN i salda kont na taśmie w zmodyfikowanym magnetowidzie. Złodziej wykorzystał te informacje, aby złupić konta klientów z innych bankomatów. Policja i Federalne Biuro Śledcze złapały złodzieja po złożonych wysiłkach detektywistycznych i inwigilacyjnych. Został skazany na 10 lat więzienia federalnego. Złodziej naruszył tajność kodów PIN klientów i sald kont, a także naruszył ich prywatność. Dostępność, użyteczność, integralność i autentyczność pozostały nienaruszone w tym naruszeniu poufności. Wyłączone posiadanie przez klientów i bank samych PIN-ów i informacji o saldzie konta zostało utracone, ale nie było ich w posiadaniu, ponieważ nadal posiadali te informacje. Dlatego był to przede wszystkim przypadek utraty poufności. Według większości ekspertów ds. bezpieczeństwa, poufność dotyczy ujawnienia, ale poufność może również zostać utracona przez obserwację, czy obserwacja ta jest dobrowolna czy mimowolna, oraz czy informacje są ujawniane lub nie są ujawniane. Na przykład, jeśli pozostawiasz wrażliwe informacje wyświetlane na ekranie monitora bez nadzoru, ujawniasz je i mogą one, ale nie muszą, utracić poufność. Jeśli wyłączysz monitor, pozostawiając pusty ekran, nie ujawniasz poufnych informacji, ale jeśli ktoś włączy monitor i odczyta jego zawartość bez pozwolenia, poufność zostanie utracona przez obserwację. Musimy zapobiec zarówno ujawnieniu, jak i obserwacji w celu ochrony poufności. Kontrola nad zachowaniem poufności obejmuje korzystanie z kryptografii, szkolenie pracowników aby stawić opór nieuczciwym atakom inżynierii społecznej, mając na celu zdobycie wiedzy technicznej i kontrolowanie korzystania z komputerów i urządzeń komputerowych. Dobre zabezpieczenie wymaga również, aby koszt zasobów na ochronę nie przekraczał wartości tego, co może zostać utracone, zwłaszcza przy niskiej częstotliwości występowania. Na przykład ochrona przed emisjami o częstotliwościach radiowych w bankomatach (jak w tym scenariuszu) prawdopodobnie nie jest wskazana, biorąc pod uwagę koszt osłony i niedostatek takich ataków high-tech. Nasilenie utraty poufności może być różne. Najgorszy scenariusz polega na tym, że strona z intencją i możliwością wyrządzenia szkody obserwuje poufne informacje ofiary. W takim przypadku może wystąpić nieodwracalne uszkodzenie. Ale informacje mogą być również znane kilku umiarkowanie szkodliwym stronom, z umiarkowanym skutkiem strat, lub mogą być znane nieszkodliwej, nieautoryzowanej stronie o krótkoterminowym odzyskiwalnym skutku.

Scenariusz straty 6: Posiadanie

Gang złodziei, wspomagany przez niezadowolonego, niedawno zwolnionego kierownika operacji, włamał się do centrum komputerowego i ukradł taśmy i dyski zawierające główne pliki firmy. Zażądali oni również kopii zapasowej i ukradli wszystkie kopie zapasowe plików. Następnie przetrzymywali materiały dla okupu w próbie wymuszenia przeciwko firmie. Włamanie spowodowało utratę przez firmę wszystkich kopii plików głównych, a także nośników, na których były przechowywane. Firma nie była w stanie kontynuować działalności biznesowej. Policja ostatecznie złapała szantażystów z pomocą firmy podczas przekazywanie okupu i odzyskała skradzione materiały. Włamywacze zostali skazani na długie kary więzienia. W tym przypadku doszło do utraty posiadania. Sprawcy opóźnili dostępność, ale firma mogła odzyskać pliki w dowolnym momencie, płacąc okup. Alternatywnie firma mogłaby ponownie utworzyć pliki główne z dokumentów papierowych, ale przy dużym koszcie. Użyteczność, integralność i autentyczność nie stanowiły problemu w tej sytuacji. Poufność nie została naruszona, ponieważ włamywacze nie mieli powodu, aby czytać lub ujawniać pliki. Utrata własności i stała utrata posiadania zostałaby dokonana, gdyby sprawcy nigdy nie zwrócili materiałów lub gdy firma przestała próbować je odzyskać. Model bezpieczeństwa musi obejmować ochronę posiadania informacji, aby

zapobiec kradzieży, niezależnie od tego, czy informacje są poufne, czy nie. Poufność z definicji dotyczy jedynie tajnych informacji, które mogą posiadać ludzie. Nasze rosnące wykorzystanie komputerów powiększa tę różnicę: ogromne ilości informacji są wykorzystywane do zautomatyzowanego użycia i niekoniecznie są utrzymywane w tajemnicy, aby tylko określone osoby mogły je znać. Programy obiektów komputerowych są przykładami zastrzeżonych, ale nie poufnych informacji, których nie znamy, sprzedając, kupując, wymieniając, dając, otrzymując i handlując, dopóki ostatecznie ich nie kontrolujemy, nie transportujemy i nie używamy. Niepoprawnie zdefiniowaliśmy posiadanie, jeśli uwzględnimy jedynie działania ochronne dotyczące materiałów poufnych. Chronimy posiadanie informacji, uniemożliwiając ludziom nieuprawnione pobieranie, wykonywanie kopii i ich przechowywanie lub kontrolowanie - niezależnie od tego, czy chodzi o poufność. Utrata posiadania informacji obejmuje także utratę kontroli nad nią i może pozwolić nowemu posiadaczowi na naruszenie jej poufności do woli. Tak więc utrata poufności może towarzyszyć utracie posiadania. Musimy jednak oddzielnie traktować poufność i posiadanie, aby określić, jakie działania mogą podjąć przestępcy i jakie kontrole musimy zastosować, aby zapobiec ich działaniom. W przeciwnym razie możemy przeoczyć konkretne zagrożenie lub skuteczną kontrolę. Niepowodzenie w przewidywaniu zagrożenia i podatności jest jednym z największych niebezpieczeństw, z jakimi mamy do czynienia w dziedzinie bezpieczeństwa. Kontrole, które mogą chronić posiadanie informacji, obejmują korzystanie z praw autorskich, wdrażanie fizycznych i logicznych ograniczeń użytkowania, konserwowanie i sprawdzanie dzienników audytu komputerowego pod kątem dowodów kradzieży, inwentaryzacji zasobów materialnych i niematerialnych, używanie wyróżniających kolorów i etykiet na pojemnikach mediów oraz przypisywanie własności do egzekwować odpowiedzialność za zasoby informacji organizacyjnych. Dotkliwość utraty posiadania różni się w zależności od charakteru przestępstwa. W najgorszym scenariuszu przestępca może pobierać informacje, a także wszystkie jego kopie, i nie może istnieć żaden sposób odzyskania środków ani od sprawcy, ani od innych źródeł, takich jak dokumentacja papierowa. W mniej szkodliwym scenariuszu przestępca może pobierać informacje przez pewien czas, ale pozostawia pewne możliwości odzyskania przy umiarkowanych kosztach. W najmniej szkodliwej sytuacji właściciel może posiadać więcej niż jedną kopię informacji, pozostawiając otwartą możliwość odzyskiwania z innych źródeł (np. Plików kopii zapasowych) w rozsądnym czasie.

WNIOSKI DOTYCZĄCE SZEŚCIU ELEMENTÓW

Musimy zrozumieć pewne ważne różnice między uczciwością i autentycznością. Po pierwsze, integralność zajmuje się wewnętrznym stanem informacji, podczas gdy autentyczność zajmuje się wartością zewnętrzną lub znaczenie w stosunku do zewnętrznych źródeł i zastosowań. Uczciwość nie dotyczy znaczenia informacji w odniesieniu do zewnętrznych źródeł, tj. tego, czy informacje są aktualne i czy nie są przestarzałe. Natomiast autentyczność dotyczy kwestii, czy informacje są prawdziwe, czy ważne i nieaktualne w odniesieniu do ich potencjalnego wykorzystania. Użytkownik, który wprowadza fałszywe informacje do komputera, może naruszył autentyczność, ale dopóki informacja pozostaje niezmieniona, ma integralność. Technolog bezpieczeństwa informacji, który projektuje zabezpieczenia w komputerowych systemach operacyjnych, dotyczy tylko integralności informacji o aplikacji, ponieważ projektant nie może wiedzieć, czy jakikolwiek użytkownik wprowadza fałszywe informacje. W takim przypadku zadaniem technologa bezpieczeństwa jest zapewnienie, że informacje prawdziwe i fałszywe pozostają kompletne. Jest to właściciel informacji, pod kierunkiem doradcy ds. bezpieczeństwa informacji, który jest odpowiedzialny za zapewnienie, że informacje są zgodne z rzeczywistością, innymi słowy, że jest autentyczny. Niektóre rodzaje strat, które musi pokonać ochrona informacji, wymagają użycia wszystkich informacji. Sześć elementów modelu ramowego w celu określenia odpowiedniego zabezpieczenia, które należy zastosować. Każdy z sześciu elementów może być naruszony niezależnie od innych, z jednym ważnym wyjątkiem: naruszenie poufności zawsze powoduje utratę wyłącznego posiadania, co najmniej. Utrata posiadania, choćby nawet wyłączne

posiadanie, niekoniecznie prowadzi do utraty poufności. Poza tym sześć elementów jest wyjątkowych i niezależnych, a często wymagają różnych zabezpieczeń. Utrzymanie dostępności informacji niekoniecznie zachowuje swoją przydatność; informacje mogą być dostępne, ale bezużyteczne w zamierzonym celu i na odwrót. Utrzymywanie integralności informacji nie musi oznaczać, że informacje są ważne, tylko że pozostają takie same lub przynajmniej pełne i kompletne. Informacja może być nieważna, a zatem bez autentyczności, ale może być obecna i identyczna z oryginalną wersją, a tym samym mieć integralność. Wreszcie, kto może przeglądać i znać informacje, a kto je posiada, to często dwie bardzo różne sprawy. Niestety, pisemne polityki bezpieczeństwa informacji wielu organizacji nie uwzględniają potrzeby zajęcia się wieloma rodzajami utraty informacji. Jest tak dlatego, że ich polityka ogranicza się do osiągnięcia CIA. Aby całkowicie zdefiniować bezpieczeństwo informacji, polityki muszą uwzględniać wszystkie przedstawione sześć elementów. Ponadto, aby wyeliminować (lub przynajmniej zmniejszyć) zagrożenia bezpieczeństwa we właściwy sposób, należy rozważyć wszystkie sześć elementów, aby zapewnić, że nic nie zostanie pominięte przy stosowaniu odpowiednich kontroli. Te elementy są również użyteczne do identyfikowania i przewidywania rodzajów działań, które przeciwnicy mogą podejmować, zanim takie działania zostaną podjęte. Dla uproszczenia i łatwości odniesienia możemy sparować sześć elementów na trzy podwójne elementy, które powinny być używane do identyfikacji zagrożeń i wybierania odpowiednich kontroli, i możemy kojarzyć je z synonimami, aby ułatwić przywoływanie i zrozumienie:

dostępność i użyteczność → użyteczność i użyteczność

integralność i autentyczność → kompletność i ważność

poufność i posiadanie → tajemnica i kontrola

Dostępność i użyteczność pasują do siebie jako pierwszy podwójny element. Elementy kontrolne wspólne dla tych elementów obejmują bezpieczną lokalizację, odpowiedni formularz do bezpiecznego użytkowania i użyteczność kopii zapasowych. Uczciwość i autentyczność również pasują do siebie; jeden dotyczy wewnętrznej struktury, a drugi - zgodności z zewnętrznymi faktami lub rzeczywistością. Kontrole dla obu obejmują podwójne wprowadzanie danych, kontrole rozsądności, użycie numerów sekwencji i sum kontrolnych lub sum kontrolnych i testy porównawcze. Kontrola zmian dotyczy również obu. Wreszcie, poufność i posiadanie idą w parze, ponieważ, jak wspomniano, są ze sobą powiązane. Powszechnie stosowane środki kontroli obejmują ochronę praw autorskich, kryptografię, podpisy cyfrowe, depozyt i bezpieczne przechowywanie. Kolejność elementów tutaj jest logiczna, ponieważ dostępność i użyteczność są niezbędne, aby integralność i autentyczność miały wartość, a te pierwsze cztery elementy są niezbędne, aby poufność i posiadanie miały istotne znaczenie.

CO SŁOWNIKI MÓWIĄ O UŻYWANYM PRZEZ NAS SŁOWIE

CIA byłaby odpowiednia dla celów bezpieczeństwa, gdyby naruszenie poufności zostało zdefiniowane jako coś, co zostało zrobione z informacją, gdyby integralność została zdefiniowana jako coś, i jeśli dostępność obejmowałaby narzędzie, ale te definicje byłyby nieprawidłowe i nie byłyby zrozumiałe dla wielu osób. Specjaliści ds. informacji definiują już termin "integralność" niepoprawnie i nie chcielibyśmy pogorszyć sytuacji. Te definicje bezpieczeństwa i elementy są odpowiednimi słownikami abstrakcji:

Bezpieczeństwo - wolność od niebezpieczeństwa, strach, niepokój, troska, niepewność, zwątpienie; podstawa zaufania; środki podjęte w celu zabezpieczenia się przed niespodziewanym atakiem, szpiegostwem, obserwacją, sabotażem; odporność kryptogramu na kryptoanalizę zwykle mierzona czasem i wysiłkiem potrzebnym do jego rozwiązania.

Dostępność - obecna lub gotowa do natychmiastowego użycia.

Użyteczność - użyteczna, przydatność do jakiegoś celu.

Stan nienaruszony- solidność; cała korespondencja z oryginalnym warunkiem; przestrzeganie kodeksu wartości moralnych, artystycznych lub innych; jakość lub stan bycia kompletnym lub niepodzielnym; materialna całość.

Autentyczność - jakość bycia autorytatywnym, ważnym, prawdziwym, prawdziwym, autentycznym, godnym akceptacji lub wiary ze względu na zgodność z faktami i rzeczywistością.

Poufność - jakość lub stan bycia prywatnym lub tajnym; znane tylko nielicznym, zawierające informacje, których nieuprawnione ujawnienie mogłoby szkodzić interesom krajowym.

Posiadanie - akt lub warunek posiadania lub brania pod kontrolę lub posiadania do dyspozycji; faktyczna fizyczna kontrola własności przez osobę, która zatrzymuje się na własność, w odróżnieniu od opieki; coś posiadanego lub kontrolowanego.

Tracimy wiarygodność i mylimy właścicieli informacji, jeśli nie używamy słów precyzyjnie i konsekwentnie. Po prawidłowym zdefiniowaniu sześć słów jest niezależnych (z wyjątkiem tego, że posiadanie informacji jest zawsze naruszane po naruszeniu poufności). Są również spójne, wyczerpujące i kompletne. Innymi słowy, wszystkie sześć elementów posiada integralność i autentyczność, a zatem mają wielką użyteczność. Nie oznacza to, że nie znajdziemy nowych elementów ani nie zastąpimy niektórych z nich w miarę rozwoju naszej wiedzy i postępów technologicznych. (Po raz pierwszy przedstawiłem demonstrację zapotrzebowania na sześć elementów w 1991 roku w XIV Amerykańskiej Agencji Bezpieczeństwa Narodowego / Krajowym Instytucie Standardów i Technologii Narodowa Konferencja Bezpieczeństwa Komputerowego w Baltimore.) Moje definicje sześciu elementów są znacznie krótsze i prostsze niż definicje słownikowe, ale odpowiednie dla bezpieczeństwa informacji

Dostępność - użyteczność informacji w określonym celu

Użyteczność - użyteczna informacji do określonego celu

Integralność - kompletność, kompletność i czytelność informacji i jakości niezmienione od poprzedniego stanu

Autentyczność - ważność, zgodność i autentyczność informacji

Poufność - ograniczona do minimum obserwacja i ujawnianie wiedzy

Posiadanie, kontrolowanie i posiadanie umiejętności korzystania z informacji

OBSZERNE LISTY ŹRÓDEŁ I CZYNNOŚCI POWODUJĄCE UTRATĘ INFORMACJI

Straty, którymi jesteśmy zaniepokojeni w dziedzinie bezpieczeństwa informacji pochodzą od ludzi, którzy angażują się w niepowołane i szkodliwe czyny skierowanych przeciwko informacji, komunikacji i systemom, takich jak malwersanci, oszuści, złodzieje, sabotażyści i źli hakerzy Angażują się w szkodliwe używanie, branie, przeinaczanie, obserwowanie i wszelkie inne wyobrażalne formy ludzkiego niewłaściwego zachowania. Naturalne siły fizyczne, takie jak ruchy powietrza i ziemi, ciepło

i zimno, energia elektromagnetyczna, żywe organizmy, grawitacja i pociski oraz woda i gazy również stanowią zagrożenie dla informacji, podobnie jak nieumyślne błędy ludzkie. Obszerne listy strat znalezionych w bezpieczeństwie informacji często obejmują oszustwo, kradzież, sabotaż i szpiegostwo, a także ujawnienie, użycie, odrzucenie i kopiowanie. Pierwsze cztery straty na tej liście są terminami wymiaru sprawiedliwości w sprawach karnych na innym poziomie abstrakcji niż cztery ostatnie i wymagają zrozumienia prawa karnego, czego wielu właścicielom informacji i specjalistom ds. Bezpieczeństwa brakuje. Na przykład oszustwo obejmuje kradzież tylko wtedy, gdy odbywa się za pomocą oszustwa, a kradzież z włamań i kradzieży z lokalu ofiary. Co stanowi "przesłanki" w środowisku sieci elektronicznej? Jest to kwestia prawna. Wiele ważnych rodzajów aktów związanych z informacjami, takich jak wprowadzanie fałszywych danych, niewykonywanie, zastępowanie, fałszowanie, wprowadzanie w błąd, przedłużanie używania, opóźnienie w użyciu, a nawet oczywiste pobieranie kopii informacji, są często pominięty na listach zdarzeń niepożądanych. Każda z tych strat może wymagać różnych kontroli zapobiegania i wykrywania. Można to łatwo przeoczyć, jeśli nasza lista potencjalnych działań jest niekompletna - nawet jeśli działania, które zazwyczaj pomijamy, należą do najczęściej zgłaszanych w rzeczywistych doświadczeniach strat. Ludzie, którzy powodują straty, często zdają sobie sprawę, że właściciele informacji nie zapewnili odpowiedniego bezpieczeństwa i nie rozważają pełnego zestawu możliwych działań. Dlatego konieczne jest uwzględnienie wszystkich rodzajów potencjalnie szkodliwych aktów na naszych listach, szczególnie gdy zastosowanie mają unikalne zabezpieczenia. W przeciwnym razie grozi nam zaniedbanie, a ci, którym odpowiadamy, będą postrzegać bezpieczeństwo informacji jako niekompletne lub źle pomyślane i wdrażane, gdy wystąpi strata. Kompletna lista aktów utraty informacji w następnej sekcji to wyczerpująca, niepełna lista potencjalnych działań powodująca straty lub informacje. Uproszczona do jednego, niskiego poziomu abstrakcji, aby ułatwić zrozumienie przez właścicieli informacji i umożliwienie im wyboru skutecznych kontroli. Lista nie rozróżnia przyczyn strat; jako taki ma on równie dobrze zastosowanie do przypadkowych i zamierzonych działań. Przyczyna jest w dużej mierze nieistotna na tym poziomie analizy bezpieczeństwa, podobnie jak jej zasadnicza intencja lub jej brak. (Identyfikacja przyczyny jest ważna na innym poziomie analizy bezpieczeństwa. Musimy określić źródła i motywację zagrożeń w celu zidentyfikowania odpowiednich mechanizmów unikania, odstraszania, korygowania i odzyskiwania). Ponadto lista nie wprowadza rozróżnienia między elektroniczną i fizyczną. przyczyny utraty lub między wypowiedzianymi, drukowanymi lub elektronicznie zapisanymi informacjami. Akty na liście pogrupowane są tak, aby odpowiadały szóstym elementom bezpieczeństwa informatycznego opisanym wcześniej (np. Dostępność i użyteczność itp.). Niektóre rodzaje działań w jednym grupowaniu elementów mogą również mieć podobny wpływ w innej grupie. Na przykład, jeśli nie istnieją żadne inne kopie informacji, zniszczenie informacji (w zależności od dostępności) może również spowodować utratę posiadania, a branie (w posiadanie) może spowodować utratę dostępności. Jednak utrata posiadania i utraty dostępności są zupełnie inne i mogą wymagać różnych kontroli. Umieściłem akty w najbardziej oczywistych kategoriach, gdzie analityk zajmujący się zapobieganiem stratom najprawdopodobniej zajrzy pierwszy. Oto skrócona wersja pełnej listy strat dla wygodnego użycia w modelu ramowym bezpieczeństwa informacji:

* Zniszczyć

* Zakłócić użycie

* Przedstaw fałszywe dane

* Zmodyfikuj lub zamień

* Fałszywe przedstawienie lub odrzucenie

PEŁNA LISTA DZIAŁAŃ DOTYCZĄCYCH UTRATY INFORMACJI

Dostępność i straty użytkowe

* Zniszczenie, uszkodzenie lub zanieczyszczenie

* Odmowa, przedłużenie, przyspieszenie lub opóźnienie w użyciu lub nabyciu

* Ruch lub niewłaściwe umieszczenie

* Konwersja lub zaciemnienie

Rzetelność i autentyczność strat

* Wstawianie, używanie lub tworzenie fałszywych lub niedopuszczalnych danych

* Modyfikacja, wymiana, usuwanie, dołączanie, agregowanie, separacja lub zmiana kolejności

* Przekręcanie

* Odrzucenie (odrzucenie jako nieprawdziwe)

* Niewłaściwe użycie lub niewykorzystanie w razie potrzeby

Poufność i straty posiadania

* Lokowanie

* Ujawnianie

* Obserwowanie, monitorowanie i pozyskiwanie

* Kopiowanie

* Bierz lub kontroluj

* Roszczenie o własność lub powiernictwo

* Wnioskowanie

* Wystawienie na wszystkie pozostałe straty

* Zagrożenie poprzez wystawienie się na jakąkolwiek inną stratę

* Niedopełnienie lub pozwolenie na wystąpienie którejkolwiek z pozostałych strat, o ile zostało to poinstruowane

Użytkownicy mogą nie znać niektórych słów na listach działań, przynajmniej w kontekście bezpieczeństwa. Na przykład "odrzucenie" to słowo, które rzadko słyszymy lub używamy poza kontekstem prawnym lub zabezpieczającym. Według słowników oznacza to odmowę uznania działań lub informacji za prawdziwe, słuszne lub z uprawnionego upoważnienia lub zobowiązania. Technolodzy bezpieczeństwa zainteresowali się odrzuceniem, gdy Massachusetts Institute of Technology (MIT) opracował bezpieczny system operacyjny sieci do użytku wewnętrznego. System nazwano Kerberos, przyjmując nazwę trójgłowego psa, który strzegł świata podziemnego w mitologii greckiej. Kerberos zapewnia środki do tworzenia bezpiecznych łączy i ścieżek między użytkownikami a komputerami, które je obsługują. Niestety, we wczesnych wersjach pozwalało to użytkownikom na fałszywe odmawianie dostępu za pomocą linków. Nie stwarzało to żadnych problemów w środowisku akademickim, ale uczyniło Kerberos niewystarczającym dla biznesu, mimo że jego inne aspekty bezpieczeństwa były atrakcyjne. Ponieważ użycie protokołu Kerberos rozprzestrzeniło się na biznes, odrzucenie stało się problemem, a kontrola nieodrzucania stała się ważna. Odmowa jest ważną kwestią

w transakcjach elektronicznych, takich jak bankowość elektroniczna, zakupy i aukcje używane przez wiele osób w celu zautomatyzowania ich funkcji zakupowych i handlu internetowego, które wymagają podpisów cyfrowych, escrow, znaczników czasu i innych kontroli uwierzytelniania. Mógłbym, na przykład, fałszywie twierdzić, że nigdy nie zamawiałem towaru i że formularz zamówienia lub przesłane elektronicznie informacje o zamówieniu, które posiada kupiec, są fałszywe. Odmowa jest również coraz większym problemem ze względu na trudność w udowodnieniu autorstwa lub źródła elektronicznych głosów. I odwrotność odrzucenia - twierdzenie, że akt, który się nie wydarzył, faktycznie się nie stało lub twierdzenie, że nieprawdziwe informacje są prawdziwe - jest również ważne dla bezpieczeństwa, chociaż często jest pomijane. Odrzucenie i jego odwrotność są obu rodzajami wprowadzenia w błąd, ale uwzględniam zarówno "odrzucenie", jak i "wprowadzenie w błąd" na liście, ponieważ mogą wymagać różnych typów kontroli. Inne słowa na liście aktów mogą wydawać się nieco niejasne. Na przykład rzadko myślisz o przedłużeniu lub opóźnieniu użycia jako o utracie dostępności lub odmowie użycia, ale są to straty, które często są powodowane przez ataki wirusów komputerowych. Używam słowa "zlokalizuj" na liście zamiast "dostęp", ponieważ dostęp może być mylący w odniesieniu do bezpieczeństwa informacji. Chociaż jest powszechnie stosowany w komputerowej terminologia, jej użycie często powoduje zamieszanie, tak jak miało to miejsce w procesie Roberta T. Morrisa dotyczącego uwolnienia robaka internetowego z 2 listopada 1988 r. oraz w przepisach dotyczących przestępczości komputerowej. Na przykład, dostęp może oznaczać po prostu pukanie do drzwi lub otwarcie drzwi, ale nie wchodzenie. Jak daleko "do" komputera trzeba iść "do niego"? Sprawca może spowodować utratę po prostu przez zlokalizowanie informacji, ponieważ właściciel może nie chcieć ujawnić posiadanie takich informacji. W tym przypadku nie ma dostępu. Z tych powodów wolę używać terminów "wejście", "wtargnięcie" i "użycie" - oraz "zlokalizuj" - odnosząc się do komputera jako przedmiotu akcji. Mam podobny problem z używaniem słowa "ujawnienie" i ignorowanie obserwacji, jak wskazałem wcześniej. "Ujawnij" to czasownik, który oznacza ujawnienie, ujawnienie, ujawnienie lub przekazanie wiedzy innym. Możemy ujawnić wiedzę poprzez:

* Nadawanie

* Mówienie

* Wyświetlanie

* Seans

* Pozostawienie go w obecności i widoku innej osoby

* Pozostawienie go w możliwym widoku, gdzie może być inna osoba

* Przekazywanie lub wysyłanie do innej osoby

Ujawnienie jest tym, co właściciel lub potencjalna ofiara może zrobić nieumyślnie lub celowo, nie to, co robi sprawca, chyba że jest to drugi akt po kradzieży, taki jak sprzedaż skradzionej własności intelektualnej innej osobie. Ujawnienie może stanowić nadużycie, jeśli osoba upoważniona do ujawnienia informacji ujawnia je nieuprawnionej osobie lub gdy nieuprawniona osoba ujawnia wiedzę innej osobie bez pozwolenia. W każdym razie poufność została utracona lub została potencjalnie utracona, a osoba ujawniająca informacje może zostać oskarżona o zaniedbanie, naruszenie prywatności, zmowę lub szpiegostwo. Utrata poufności może również nastąpić w wyniku obserwacji, czy ofiara lub właściciel ujawnił wiedzę, przeciwstawić się ujawnieniu lub nie uczynić nic, aby go chronić lub ujawnić. Obserwowanie jest nadużyciem słuchania, szpiegowania poprzez podsłuchiwanie, surfowanie po ramieniu (patrzenie na ramię innej osoby lub podsłuchiwanie), oglądanie lub słuchanie skradzionej kopii informacji, lub nawet przez dotykowe uczucie, jak w przypadku czytania brajla.

Powinniśmy pomyśleć o utracie poufności jako straty spowodowanej przez nieumyślne ujawnienie przez ofiarę, obserwację sprawcy i ujawnienie przez sprawcę, który przekazuje informacje stronie trzeciej. Ujawnienie i obserwacja informacji, która nie jest wiedzą, zamienia ją w wiedzę, jeśli ma miejsce poznawanie. Ujawnienie zawsze prowadzi do utraty poufności poprzez umieszczenie informacji w stanie, w którym nie ma już tajemnicy, ale obserwacja prowadzi do utraty poufności tylko wtedy, gdy ma miejsce poznanie lub wykorzystanie na niekorzyść właściciela. Prywatność to prawo, które jest zupełnie innym tematem, którego tutaj nie omawiam. Utrata posiadania informacji (w tym wiedzy) jest utratą z niezamierzonego lub żałosnego dawania lub odbierania informacji. Na wyższym poziomie opisu przestępstwa nazywamy to kradzieżą (kradzieżą lub włamaniem) lub oszustwem (w przypadku oszustwa). Posiadanie wydaje się być najbardziej ściśle związane z poufnością. Oba są umieszczone razem na liście, ponieważ mają one wspólne straty związane z przyjmowaniem i kopiowaniem (utrata wyłącznego posiadania). Mógłbym użyć "własności" informacji, ponieważ jest to synonim posiadania, ale "własność" wydaje się być nie tak szeroka, ponieważ ktoś może słusznie lub niesłusznie posiadać informacje, które są prawnie własnością innego. Koncepcje właściciela lub posiadacza informacji, wraz z użytkownikiem, dostawcą lub depozytariuszem informacji, są ważnymi rozróżnieniami w zakresie bezpieczeństwa dla przypisania odpowiedzialności za aktywa. Zapewnia to kolejny powód umieszczenia posiadania na liście. Akt zagrożenia jest zupełnie inny, ale odnosi się do innych strat. Oznacza to umieszczanie informacji w szkodliwy sposób lub, że dana osoba została usunięta (i prawdopodobnie zaniedbana), nie stosując wystarczającej ochrony informacji, takich jak pozostawienie wrażliwych lub wartościowych dokumentów w otwartym biurze lub otwartym koszu. Pozostawienie komputera niepotrzebnie połączonego z Internetem to kolejny przykład. Zagrożenie informacjami może prowadzić do zarzutów zaniedbania lub zaniedbań karnych oraz pozwów o odpowiedzialność cywilną, które mogą być droższe niż bezpośrednie straty. Moje cele bezpieczeństwa w modelu ramowym wymaga standardu należytej staranności, aby poradzić sobie z tym narażeniem. Ostatni akt na liście - brak zaangażowania lub zezwolenia na inne działania, kiedy poinstruowany, aby to zrobić - na pierwszy rzut oka może wydawać się dziwny. Oznacza to, że właściciel informacji może wymagać czynności powodującej wykonanie któregokolwiek z pozostałych działań. Lub właściciel może życzyć sobie, aby dopuszczono do popełnienia czynu, lub informacji, które mogą zagrozić stratą. Istnieją sytuacje, w których informacja powinna być narażona na szkody dla celów testowania lub dla osiągnięcia większego dobra. Na przykład programiści komputerowi i audytorzy często tworzą pliki informacyjne, które są celowo nieważne do użycia jako dane wejściowe do komputera w celu upewnienia się, że kontrole służące do wykrywania lub łagodzenia utraty działają poprawnie. Programista nastawiony na przestępczość może usunąć niepoprawne dane w pliku wejściowym testu, aby uniknąć testowania kontroli, którą sprawca zneutralizował lub uniknął implementacji w niecnych celach. Lista ta byłaby z pewnością niekompletna bez tego rodzaju straty, ale nigdy nie widziałem jej w żadnym innym tekście bezpieczeństwa informacji. Akty na liście są opisane na odpowiednim poziomie do określenia i określenia odpowiednich środków kontroli w zakresie ochrony. Przy następnym niższym poziomie abstrakcji (np. Odczyt, zapis i wykonanie) straty nie byłyby tak oczywiste i niekoniecznie sugerowałyby ważne kontrole. Na poziomie, który wybieram, nie próbuję rozróżniać aktów, które nie zmieniają informacji od tych, które robią, ponieważ różnice te nie są istotne dla identyfikacji bezpośrednio stosowanych kontroli lub do przeprowadzania analiz zagrożeń. Na przykład akt zmiany modyfikacji informacje, podczas gdy akt obserwacji tego nie robi, ale szyfrowanie może być wykorzystane jako potężna podstawowa kontrola przeciwko obu działaniom.

PRZYKŁADY DZIAŁANIA I SUGEROWANYCH KONTROLI

Kolejne przykłady ilustrują związki między aktami i kontrolami w analizie zagrożeń. Po grupach aktów następują przykłady strat i stosownych kontroli.

ZNISZCZENIE, USZKODZENIE LUB ZANIECZYSZCZENIE

Sprawcy lub szkodliwe siły mogą uszkodzić, zniszczyć lub zanieczyścić informacje przez elektroniczną kasę, pisząc nad nimi inne dane, stosując wysokoenergetyczne fale radiowe, aby uszkodzić delikatne układy elektroniczne lub fizycznie uszkadzając media (np. Papier, pamięć flash lub dyski) zawierające go. Kontrole obejmują zabezpieczenia przed awarią, takie jak zablokowane urządzenia, bezpieczne przechowywanie kopii zapasowych i wymagania dotyczące autoryzacji użycia zapisu.

ZAPRZECZANIE, PRZEDŁUŻANIE, OPÓŹNIANIE UŻYCIA LUB POZYSKANIE

Sprawcy mogą uczynić informację niedostępną, ukrywając ją lub odmawiając jej użycia za pomocą szyfrowania i nie ujawniając środków do jej przywrócenia lub utrzymując krytyczne jednostki przetwarzające zajęte innymi działaniami, na przykład podczas ataku typu "odmowa usługi". Takie działania niekoniecznie niszczą informacje. Podobnie sprawca może przedłużyć korzystanie z informacji, wprowadzając zmiany programowe spowalniające przetwarzanie w komputerze lub spowalniając wyświetlanie informacji na ekranie. Takie działania mogą spowodować nieakceptowalny czas na skuteczne wykorzystanie informacji. Pozyskiwanie informacji może być opóźnione przez wymaganie zbyt wielu hasła, aby je odzyskać lub spowalniając pobieranie. Te działania mogą sprawić, że informacje staną się przestarzałe do czasu, kiedy staną się dostępne. Kontrole obejmują udostępnianie wielu kopii z różnych źródeł, zapobieganie przeciążeniu przetwarzania poprzez selektywne uwzględnianie danych wejściowych lub uniemożliwianie aktywacji szkodliwe mechanizmy, takie jak wirusy komputerowe za pomocą narzędzi antywirusowych.

WPROWADZENIE, UŻYWANIE LUB TWORZENIE FAŁSZYWYCH DANYCH

Drone danych, mój termin na fałszywe wprowadzanie danych i ich używanie, jest powszechną formą przestępczości komputerowej, która liczy oszustwa finansowe i związane z nimi straty. Straty mogą być celowe, na przykład wynikające z użycia koni trojańskich (w tym wirusów komputerowych) lub niezamierzone, na przykład z powodu błędów wejściowych. Większość wewnętrznych kontroli, takich jak kontrola zasięgu, drogi audytu, rozdział obowiązków, zduplikowane wykrywanie wprowadzania danych, sprawdzanie programu i sumy kontrolne dla elementów danych chronią przed tymi zagrożeniami.

MODYFIKUJ , ZAMIENIAJ LUB ZMIENIAJ KOLEJNOŚĆ

Akty te są często inteligentnymi zmianami, a nie uszkodzeniem lub zniszczeniem. Zmiana kolejności, która w rzeczywistości jest formą modyfikacji, jest zawarta osobno, ponieważ może wymagać konkretnych kontroli, które w przeciwnym razie mogłyby zostać przeoczone. Podobnie uwzględniono wymianę, ponieważ użytkownicy nie mogliby w inny sposób wymieniać całego pliku danych podczas rozważania modyfikacji. Każde z tych działań może spowodować utratę nieodłączną dla zagrożeń związanych z wprowadzaniem i modyfikowaniem informacji, ale w tym wszystkie obejmują modyfikację danych zarówno przed wprowadzeniem, jak i po wprowadzeniu, ponieważ każda z nich wymaga innej kontroli. Kryptografia, podpisy cyfrowe, autoryzacja użytkowania i sekwencjonowanie wiadomości są przykładami kontroli, które mają na celu ochronę przed takimi aktami, a także kontrole wykrywania w celu identyfikacji anomalii.

FAŁSZYWE PZEDSTAWIENIE

Twierdzenie, że informacje są czymś różnym od tego, czym jest naprawdę lub ma inne znaczenie od tego, co było zamierzone, w sfałszowaniu, fałszerstwach, oszustwach, podszywaniu się pod inne osoby (upoważnionych użytkowników) i wielu innych oszukańczych działaniach. Hakerzy używają fałszywych informacji w inżynierii społecznej, by zwieść ludzi w celu ujawnienia informacji potrzebnych do

atakowania systemów. Nieprawidłowa prezentacja starych danych jako nowych informacji to kolejna tego typu czynność. Formanty obejmują metody uwierzytelniania użytkowników i dokumentów, takie jak hasła, podpisy cyfrowe i testy poprawności danych. Sprawienie, by zaufani ludzie byli bardziej odporni na oszustwo dzięki przypomnieniom i szkoleniom, to kolejna kontrola.

ODRZUCENIE

Ten rodzaj straty, w którym sprawcy zazwyczaj zaprzeczają istnieniu dokonane transakcje są powszechne w elektronicznej wymianie danych (EDI) i handlu elektronicznym. Negowanie przez Olivera Northa treści jego e-maili jest godnym uwagi przykładem odrzucenia, ale jak już wspomniałem wcześniej, odwrotność odrzucenia również oznacza potencjalną stratę. Odrzucanie można najskuteczniej kontrolować za pomocą podpisów cyfrowych i kryptografii klucza publicznego. Zaufane strony trzecie, takie jak urzędy certyfikacji z bezpiecznymi serwerami komputerowymi, zapewniają niezależność notariusza, aby stawiały opór odmowy dostępu prawdziwe informacje, o ile mogą zostać pociągnięte do odpowiedzialności za swoje niepowodzenia.

NIEWŁAŚCIWE UŻYCIE LUB NIEPRAWIDŁOWE UŻYCIE

Niewłaściwe wykorzystanie informacji jest wyraźnie czynnością powodującą wiele strat informacji. Niewłaściwe użycie przez niewykonanie takich obowiązków ponieważ aktualizowanie plików lub tworzenie kopii zapasowych informacji nie jest tak oczywiste i wymaga jednoznacznej identyfikacji. Niejawne niewłaściwe użycie przez dokładne dostosowanie do nieodpowiednich lub nieprawidłowych instrukcji jest pewnym sposobem na sabotowanie systemów. Kontrola użycia informacji i wewnętrzne kontrolki aplikacji, które ograniczają modyfikację lub używanie zaufanego oprogramowania, pomagają uniknąć tych problemów. Prowadzenie bezpiecznych dzienników rutynowych czynności może pomóc w złapaniu operacyjnych luk.

ZLOKALIZUJ

Nieuprawnione użycie czyjegoś komputera lub sieci danych do zlokalizowania i identyfikacji informacji jest przestępstwem w większości przypadków przestępstw komputerowych - nawet jeśli nie ma jawnej intencji spowodowania szkody. Takie korzystanie jest naruszeniem prywatności, a naruszenie prawa do takiego użytkowania jest przestępstwem na mocy innych przepisów. Kontrolki logowania i użytkowania są głównymi funkcjami w wielu systemach operacyjnych, takich jak Microsoft Windows i niektóre wersje systemu UNIX, a także w dodatkowych narzędziach bezpieczeństwa, takich jak RACF i ACF2 dla dużych komputerów IBM i wielu produktów bezpieczeństwa dla komputerów osobistych.

UJAWNIENIE

Zapobieganie ujawnianiu informacji osobom nieupoważnionym do tego jest celem tajemnicy służbowej, osobistej i rządowej. Ujawnienie może być ustne, pocztą lub poprzez przesłanie wiadomości lub plików w formie elektronicznej lub na dyskach, pamięciach flash lub taśmie. Ujawnienie może spowodować utratę prywatności i tajemnice handlowe. Organizacje wojskowe mają zaawansowaną ochronę poufności informacji w skomplikowanej formie sztuki.

OBSERWUJ LUB MONITORUJ

Obserwacja, która wymaga działania ze strony sprawcy, jest odwrotnością ujawnienia, która wynika z działań posiadacza. Ekrany wyświetlacza stacji roboczych, linie komunikacyjne i urządzenia monitorujące, takie jak rejestratory i dzienniki audytu są wspólnymi celami obserwacji i monitorowania. Obserwacja wyników z drukarek jest kolejnym możliwym źródłem, podobnie jak surfowanie po ramieniu - technika oglądania ekranów innych użytkowników komputerów. Fizyczna

ochrona wejścia dla urządzeń wejściowych i wyjściowych stanowi główną kontrolę zapobiegającą tego rodzaju utracie. Ważne jest także zapobieganie podsłuchom i podsłuchom.

KOPIUJ

Kopiarka i polecenie kopiowania oprogramowania są głównymi źródłami nieautoryzowanego kopiowania. Kopiowanie jest wykorzystywane do naruszania wyłącznego posiadania i prywatności. Kopiowanie może niszczyć autentyczność, tak jak w przypadku fałszowania pieniędzy lub innych instrumentów biznesowych. Kontrole dotyczące lokalizacji i użytkowania są skuteczne w stosunku do kopiowania, podobnie jak unikalne oznaczenia, takie jak te używane w walucie USA i znaki wodne na papierze iw plikach komputerowych.

WEŹ

Przesyłanie plików danych w komputerach lub sieciach stanowi pobieranie. Tak samo jest z przyjmowaniem małych komputerów i DVD lub dokumentów dla wartości przechowywanych w nich informacji. Sprawcy mogą bez problemu pobrać kopie informacji pozbawienie właściciela posiadania lub poufności. Do tych strat stosuje się szeroki zakres fizycznych i logicznych mechanizmów kontroli lokalizacji; większość opiera się na zdrowym rozsądku i rozsądnym poziomie należytej staranności.

ZAGROŻENIE

Umieszczenie informacji w miejscach lub warunkach, w których inni mogą spowodować utratę w którymkolwiek z opisanych wcześniej sposobów, wyraźnie zagraża informacji, a sprawca może zostać oskarżony o zaniedbanie. Istotne są fizyczne i logiczne środki zapobiegania niebezpieczeństwu. Szkolenie ludzi do zachowania ostrożności i pociąganie ich do odpowiedzialności za ochronę informacji może być najskuteczniejszym sposobem zapobiegania zagrożeniom

INFORMACJE FIZYCZNE U STRATY SYSTEMÓW

Informacje mogą również cierpieć z powodu strat fizycznych, takich jak powodzie, trzęsienia ziemi, promieniowanie i pożary. Chociaż straty te nie wpływają bezpośrednio na same informacje (np. znajomość procedur operacyjnych przechowywanych w głowach operatorów), mogą uszkodzić lub zniszczyć media i środowisko, które zawierają reprezentacje informacji. Na przykład woda może niszczyć wydrukowane strony i uszkadzać dyski magnetyczne; fizyczne drgania lub promieniowanie o częstotliwości radiowej może powodować zwarcie obwodów elektronicznych, a pożary mogą niszczyć wszystkie rodzaje mediów. Ogólnie rzecz biorąc, straty fizyczne mogą wystąpić na siedem naturalnych sposobów poprzez zastosowanie:

1. Ekstremalna temperatura

2. Gazy

3. Ciecze

4. Organizmy żywe

5. Pociski

6. Ruchy

7. Anomalie energetyczne

Każdy sposób, oczywiście, pochodzi z konkretnych źródeł strat (np. Dymu lub wody). I różne sposoby można dalej rozbić, aby zidentyfikować podstawową przyczynę źródła strat. Na przykład cieczą, która

niszczy informacje, może być woda płynąca z przerwy hydraulicznej nad stanowiskiem komputerowym, wywołana z kolei przez mroźną pogodę. Następna lista przedstawia przykłady każdego z siedmiu głównych źródeł strat fizycznych.

1. Ekstremalna temperatura. Ciepło lub zimno. Przykłady: światło słoneczne, ogień, mróz, upał i rozkład urządzeń klimatyzacyjnych.

2. Gazy. Gazy bojowe, opary komercyjne, wilgotne lub suche powietrze, zawieszone cząstki. Przykłady: gaz nerwowy sarin, PCB z eksplodujących transformatorów, uwolnienie freonu z klimatyzatorów, dym i smog, płyn czyszczący i opary paliwa.

3. Ciecze. Woda, chemikalia. Przykłady: powodzie, awarie hydrauliczne, opady, wycieki paliwa, rozlane napoje, kwaśne i podstawowe substancje chemiczne używane do czyszczenia oraz płyny do drukarek komputerowych.

4. Organizmy żywe. Wirusy, bakterie, grzyby, rośliny, zwierzęta i ludzie. Przykłady: choroby kluczowych pracowników, pleśnie, zanieczyszczenia z olejków skórnych i włosów, zanieczyszczenia i elektryczne zwarcia od wypróżniania i uwalniania płynów ustrojowych, zużycie mediów informacyjnych, takich jak papier lub izolacja kabli, oraz zwarcie mikroukładów z pajęczyny.

5. Pociski. Namacalne obiekty w ruchu, zasilane obiekty. Przykłady: meteoryty, spadające obiekty, samochody i ciężarówki, samoloty, pociski i rakiety, eksplozje i wiatry.

6. Ruch. Zapadnij, strzyżenie, drżenie, wibracje, upłynnienia, przepływy, fale, separacja, slajdy. Przykłady: upuszczenie lub potrząsanie delikatnym sprzętem, trzęsienia ziemi, slajdy ziemi, przepływy lawy, fale morskie i błędy adhezyjne.

7. Anomalie energetyczne. Udar lub awarie elektryczne, magnetyzm, elektryczność statyczna, obwody starzenia; promieniowanie, dźwięk, światło, radio, mikrofale, elektromagnetyczne, atomowe. Przykłady: awarie urządzeń elektrycznych, bliskość magnesów i elektromagnesów, statyczne wykładziny dywanowe, impulsy elektromagnetyczne (EMP) z wybuchów jądrowych, lasery, głośniki, wysokoenergetyczne działa radiowe (HERF), systemy radarowe, promieniowanie kosmiczne i wybuchy.

Chociaż na przykład meteoryty stanowią niewielkie zagrożenie dla komputerów, ważne jest, aby uwzględnić wszystkie takie nieprawdopodobne zdarzenia w dokładnej analizie potencjalnych zagrożeń. Ogólnie rzecz ujmując, uwzględnij wszystkie możliwe działania uwzględnione w analizie zagrożeń. Następnie rozważ to ostrożnie; jeśli jest to zbyt mało prawdopodobne, udokumentuj rozpatrzenie i odrzuć przedmiot. Lepiej jest pomyśleć o źródle straty i wyrzucić ją, niż przeoczyć ważną. Niezmiennie, gdy przedstawisz analizę zagrożeń innym, ktoś spróbuje zaskoczyć programistę innym źródłem straty, które zostało przeoczone. Niewyczerpani praktycy od samego początku posiadali niewystarczające listy strat w zasobach wiedzy od samego początku bezpieczeństwa informacji. Proponowanie poważnej zmiany w tak późnym terminie jest odważną akcją, która może zająć dużo czasu. Nie wolno nam jednak utrwalać naszych przeszłych niedociągnięć, wykorzystując obecnie przyjęte zniszczenie, ujawnienie, użycie i modyfikację (DDUM) jako pełną listę strat. Nie możemy podważać lub upraszczać złożoność naszego przedmiotu kosztem wprowadzających w błąd właścicieli informacji. Nasi przeciwnicy zawsze szukają słabości w bezpieczeństwie informacji, ale naszą siłą jest przewidywanie źródeł zagrożeń i posiadanie planów zapobiegających stratom, które mogą powodować. Nie można zebrać naprawdę kompletnej listy źródeł utraty informacji, które mogą być spowodowane przez zamierzone lub przypadkowe działania ludzi. Naprawdę nie mamy pojęcia, co ludzie mogą robić - teraz lub w przyszłości. Opieramy nasze listy na doświadczeniach, ale dopóki nie będziemy w stanie wyobrazić sobie jakiegoś aktu, lub dopóki nie pojawi się zagrożenie lub nie pojawi się zagrożenie, nie możemy

włączyć go do listy. A nieznajomość zagrożenia oznacza, że nie możemy opracować planu ochrony przed nim. Jest to jeden z powodów, dla których bezpieczeństwo informacji jest nadal sztuką ludową, a nie nauką.

FUNKCJE BEZPIECZEŃSTWA INFORMACJI

Zaproponowany model bezpieczeństwa informacji obejmuje 12 funkcji bezpieczeństwa zamiast 3 (zapobieganie, wykrywanie i odzyskiwanie) zawartych w poprzednich modelach. Funkcje te opisują działania podejmowane przez praktyków bezpieczeństwa informacji i właścicieli informacji w celu ochrony informacji, a także cele stosowanych przez nich zabezpieczeń. Każda kontrola obsługuje jedną lub więcej z tych funkcji. Chociaż niektórzy specjaliści ds. bezpieczeństwa dodają inne funkcje do listy, takie jak zapewnienie jakości i niezawodność, uważam, że nie mieszczą się one w zakresie bezpieczeństwa informacji; inne wyspecjalizowane pola zajmują się nimi. Niezawodność jest trudna w odniesieniu do bezpieczeństwa, z wyjątkiem zagrożenia, gdy sprawcy niszczą wiarygodność informacji i systemów, co stanowi naruszenie bezpieczeństwa. Tak więc bezpieczeństwo musi zachować stan niezawodności, ale nie musi koniecznie próbować go poprawić. Bezpieczeństwo musi chronić możliwość audytowania informacji i systemów, a jednocześnie samo bezpieczeństwo musi być wiarygodne i podlegać audytowi. Uważam, że moje definicje bezpieczeństwa obejmują niszczenie niezawodności i audytowności informacji na wysokim poziomie abstrakcji. Na przykład rzetelność zmniejsza się, gdy kwestionuje się autentyczność informacji, zmieniając ją z właściwej reprezentacji faktu. Podobnie, nie uwzględniam takich funkcji, jak uwierzytelnianie użytkowników i weryfikacja na moich listach, ponieważ uważam je za cele kontroli w celu osiągnięcia 12 funkcji bezpieczeństwa informacji. Istnieje wyraźna logika w kolejności, w której przedstawiam 12 funkcji na liście. Metodyczny praktyk bezpieczeństwa informacji może zastosować funkcje w tej kolejności podczas rozwiązywania luk w zabezpieczeniach.

1. Bezpieczeństwo informacji musi być najpierw poddane niezależnemu audytowi w sposób kontradyktoryjny w celu udokumentowania jego stanu oraz zidentyfikowania jego słabości i mocnych stron.

2. Praktyk musi ustalić, czy można całkowicie uniknąć problemu związanego z bezpieczeństwem.

3. Jeśli problemu nie można uniknąć, praktyk musi postarać się powstrzymać potencjalnych nadużywających lub siły od niewłaściwego zachowania.

4. Jeśli zagrożenia nie da się uniknąć lub zniechęcić, praktyk próbuje wykryć jego aktywację.

5. Jeżeli wykrycie nie jest zapewnione, wówczas praktyk stara się zapobiec wystąpieniu tego aktu.

6. Jeśli zapobieganie się nie powiedzie i nastąpi działanie, wówczas praktyk musi je zatrzymać lub zminimalizować jego szkodliwe skutki poprzez łagodzenie.

7. Praktyk musi ustalić, czy przeniesienie odpowiedzialności na inną osobę lub dział może być bardziej skuteczne w rozwiązywaniu sytuacji wynikającej z ataku, lub jeśli inna strona (np. Ubezpieczyciel) może zostać pociągnięta do odpowiedzialności za koszt straty.

8. Po wystąpieniu straty, praktyk musi zbadać i wyszukać osobę (osoby) lub siłę (siły), która spowodowała lub przyczyniła się do incydentu, a także wszystkie strony, które odegrały w nim rolę - pozytywnie lub negatywnie.

9. Po ustaleniu, wszystkie strony powinny być odpowiednio ukarane lub nagrodzone.

10. Po zakończeniu incydentu ofiara musi odzyskać lub asystować przy odzyskaniu

11. Interesariusze powinni podjąć działania korygujące, aby zapobiec ponownemu wystąpieniu tego samego rodzaju incydentu.

12. Zainteresowane strony muszą uczyć się na doświadczeniu, aby pogłębić swoją wiedzę na temat bezpieczeństwa informacji i edukować innych

WYBÓR ZABEZPIECZEŃ PRZY UŻYCIU STANDARDU NALEŻYTEJ STARANNOŚCI

Praktycy bezpieczeństwa informacji zwykle odnoszą się do procesu wyboru zabezpieczeń, takich jak ocena ryzyka, analiza ryzyka lub zarządzanie ryzykiem. Wybory zabezpieczeń opartych na ryzyku obliczenia mogą być bezowocnym i kosztownym procesem. Chociaż wielu ekspertów i stowarzyszeń zajmujących się bezpieczeństwem zaleca stosowanie metod oceny ryzyka, wiele organizacji ostatecznie odkrywa, że stosowanie standardu należytej staranności (lub opieki) jest o wiele lepsze i bardziej praktyczne. Często jedno smutne doświadczenie związane z oceną ryzyka bezpieczeństwa wystarcza, aby przekonać departamenty bezpieczeństwa informacji i korporacyjne do zarządzania ich ograniczeniami. Ryzyko bezpieczeństwa jest funkcją prawdopodobieństwa lub częstotliwości występowania rzadkich zdarzeń strat i ich skutków, a żadne z nich nie jest dostatecznie mierzalne ani przewidywalne dla inwestycji w bezpieczeństwo. Pamiętaj, że ryzyko dotyczy tylko rzadkich zdarzeń. Zdarzenia takie jak ataki wirusów komputerowych lub oszustwa związane z kartami kredytowymi występują w sposób ciągły i nie stanowią zagrożenia; są pewni i mogą być mierzone, kontrolowane i zarządzane. Standard metody należytej staranności jest prosty i oczywisty; jest domyślny proces, który zalecam i który jest powszechnie stosowany dzisiaj zamiast bardziej rozbudowanych podejść "naukowych". Standard uznawania należytej staranności jest uznawany i akceptowany przez wiele dokumentów prawnych i organizacji i jest udokumentowane w licznych przewodnikach biznesowych.

FUNKCJE BEZPIECZEŃSTWA INFORMACJI

Zaproponowany model bezpieczeństwa informacji obejmuje 12 funkcji bezpieczeństwa zamiast 3 (zapobieganie, wykrywanie i odzyskiwanie) zawartych w poprzednich modelach. Funkcje te opisują działania podejmowane przez praktyków bezpieczeństwa informacji i właścicieli informacji w celu ochrony informacji, a także cele stosowanych przez nich zabezpieczeń. Każda kontrola obsługuje jedną lub więcej z tych funkcji. Chociaż niektórzy specjaliści ds. bezpieczeństwa dodają inne funkcje do listy, takie jak zapewnienie jakości i niezawodność, uważam, że nie mieszczą się one w zakresie bezpieczeństwa informacji; inne wyspecjalizowane pola zajmują się nimi. Niezawodność jest trudna w odniesieniu do bezpieczeństwa, z wyjątkiem zagrożenia, gdy sprawcy niszczą wiarygodność informacji i systemów, co stanowi naruszenie bezpieczeństwa. Tak więc bezpieczeństwo musi zachować stan niezawodności, ale nie musi koniecznie próbować go poprawić. Bezpieczeństwo musi chronić możliwość audytowania informacji i systemów, a jednocześnie samo bezpieczeństwo musi być wiarygodne i podlegać audytowi. Uważam, że moje definicje bezpieczeństwa obejmują niszczenie niezawodności i audytowności informacji na wysokim poziomie abstrakcji. Na przykład rzetelność zmniejsza się, gdy kwestionuje się autentyczność informacji, zmieniając ją z właściwej reprezentacji faktu. Podobnie, nie uwzględniam takich funkcji, jak uwierzytelnianie użytkowników i weryfikacja na moich listach, ponieważ uważam je za cele kontroli w celu osiągnięcia 12 funkcji bezpieczeństwa informacji. Istnieje wyraźna logika w kolejności, w której przedstawiam 12 funkcji na liście. Metodyczny praktyk bezpieczeństwa informacji może zastosować funkcje w tej kolejności podczas rozwiązywania luk w zabezpieczeniach.

1. Bezpieczeństwo informacji musi być najpierw poddane niezależnemu audytowi w sposób kontradyktoryjny w celu udokumentowania jego stanu oraz zidentyfikowania jego słabości i mocnych stron.

2. Praktyk musi ustalić, czy można całkowicie uniknąć problemu związanego z bezpieczeństwem.

3. Jeśli problemu nie można uniknąć, praktyk musi postarać się powstrzymać potencjalnych nadużywających lub siły od niewłaściwego zachowania.

4. Jeśli zagrożenia nie da się uniknąć lub zniechęcić, praktyk próbuje wykryć jego aktywację.

5. Jeżeli wykrycie nie jest zapewnione, wówczas praktyk stara się zapobiec wystąpieniu tego aktu.

6. Jeśli zapobieganie się nie powiedzie i nastąpi działanie, wówczas praktyk musi je zatrzymać lub zminimalizować jego szkodliwe skutki poprzez łagodzenie.

7. Praktyk musi ustalić, czy przeniesienie odpowiedzialności na inną osobę lub dział może być bardziej skuteczne w rozwiązywaniu sytuacji wynikającej z ataku, lub jeśli inna strona (np. Ubezpieczyciel) może zostać pociągnięta do odpowiedzialności za koszt straty.

8. Po wystąpieniu straty, praktyk musi zbadać i wyszukać osobę (osoby) lub siłę (siły), która spowodowała lub przyczyniła się do incydentu, a także wszystkie strony, które odegrały w nim rolę - pozytywnie lub negatywnie.

9. Po ustaleniu, wszystkie strony powinny być odpowiednio ukarane lub nagrodzone.

10. Po zakończeniu incydentu ofiara musi odzyskać lub asystować przy odzyskaniu

11. Interesariusze powinni podjąć działania korygujące, aby zapobiec ponownemu wystąpieniu tego samego rodzaju incydentu.

12. Zainteresowane strony muszą uczyć się na doświadczeniu, aby pogłębić swoją wiedzę na temat bezpieczeństwa informacji i edukować innych

WYBÓR ZABEZPIECZEŃ PRZY UŻYCIU STANDARU NALEŻYTEJ STARANNOŚCI

Praktycy bezpieczeństwa informacji zwykle odnoszą się do procesu wyboru zabezpieczeń, takich jak ocena ryzyka, analiza ryzyka lub zarządzanie ryzykiem. Wybory zabezpieczeń opartych na ryzyku obliczenia mogą być bezowocnym i kosztownym procesem. Chociaż wielu ekspertów i stowarzyszeń zajmujących się bezpieczeństwem zaleca stosowanie metod oceny ryzyka, wiele organizacji ostatecznie odkrywa, że stosowanie standardu należytej staranności (lub opieki) jest o wiele lepsze i bardziej praktyczne. Często jedno smutne doświadczenie związane z oceną ryzyka bezpieczeństwa wystarcza, aby przekonać departamenty bezpieczeństwa informacji i korporacyjne do zarządzania ich ograniczeniami. Ryzyko bezpieczeństwa jest funkcją prawdopodobieństwa lub częstotliwości występowania rzadkich zdarzeń strat i ich skutków, a żadne z nich nie jest dostatecznie mierzalne ani przewidywalne dla inwestycji w bezpieczeństwo. Pamiętaj, że ryzyko dotyczy tylko rzadkich zdarzeń. Zdarzenia takie jak ataki wirusów komputerowych lub oszustwa związane z kartami kredytowymi występują w sposób ciągły i nie stanowią zagrożenia; są pewni i mogą być mierzone, kontrolowane i zarządzane. Standard metody należytej staranności jest prosty i oczywisty; jest domyślny proces, który zalecam i który jest powszechnie stosowany dzisiaj zamiast bardziej rozbudowanych podejść "naukowych". Standard uznawania należytej staranności jest uznawany i akceptowany przez wiele dokumentów prawnych i organizacji i jest udokumentowane w licznych przewodnikach biznesowych.

ZAGROŻENIA, AKTYWA, MODEL WARTOŚCI

Łączenie wszystkich aspektów w jednym miejscu jest użytecznym sposobem analizy zagrożeń bezpieczeństwa i słabych punktów oraz tworzenia skutecznych scenariuszy testowania rzeczywistych systemów informatycznych i organizacji. Użytkownicy mogą nakreślić scenariusz lub przeanalizować

prawdziwy przypadek, okrążając i łącząc odpowiednie n w każdej kolumnie modelu. W tej wersji modelu kolumna Kontrolki zawiera tylko nagłówki tematów rodzaje kontroli; ukończony model zawierałby setki kontroli. Jeśli model jest używany do przeprowadzenia przeglądu, sugeruję, aby sekcja "Podatności" modelu została zmieniona na "Zalecane kontrole".

WNIOSEK

Ramy bezpieczeństwa zaproponowane w tym rozdziale stanowią próbę przezwyciężenia dominującego poglądu technologa na bezpieczeństwo informacji poprzez skupienie się w szerszym zakresie na wszystkich aspektach bezpieczeństwa, w tym na informacjach, które próbujemy chronić, potencjalnych źródłach strat, rodzajach strat, kontrole, które możemy zastosować, aby uniknąć strat, metody wyboru tych kontroli i nasze ogólne cele w zakresie ochrony informacji. Ta szeroka perspektywa powinna przynieść dwa korzystne efekty: zwiększyć bezpieczeństwo informacji od wąskiej sztuki ludowej do szerokiej dyscypliny, a przede wszystkim pomóc w ograniczeniu wielu strat związanych z informacją, niezależnie od tego, gdzie ona istnieje.

ZAGROŻENIA, AKTYWA, MODEL WARTOŚCI

Łączenie wszystkich aspektów w jednym miejscu jest użytecznym sposobem analizy zagrożeń bezpieczeństwa i słabych punktów oraz tworzenia skutecznych scenariuszy testowania rzeczywistych systemów informatycznych i organizacji. Użytkownicy mogą nakreślić scenariusz lub przeanalizować prawdziwy przypadek, okrążając i łącząc odpowiednie n w każdej kolumnie modelu. W tej wersji modelu kolumna Kontrolki zawiera tylko nagłówki tematów rodzaje kontroli; ukończony model zawierałby setki kontroli. Jeśli model jest używany do przeprowadzenia przeglądu, sugeruję, aby sekcja "Podatności" modelu została zmieniona na "Zalecane kontrole".

WNIOSEK

Ramy bezpieczeństwa zaproponowane tu stanowią próbę przezwyciężenia dominującego poglądu technologa na bezpieczeństwo informacji poprzez skupienie się w szerszym zakresie na wszystkich aspektach bezpieczeństwa, w tym na informacjach, które próbujemy chronić, potencjalnych źródłach strat, rodzajach strat, kontrole, które możemy zastosować, aby uniknąć strat, metody wyboru tych kontroli i nasze ogólne cele w zakresie ochrony informacji. Ta szeroka perspektywa powinna przynieść dwa korzystne efekty: zwiększyć bezpieczeństwo informacji od wąskiej sztuki ludowej do szerokiej dyscypliny, a przede wszystkim pomóc w ograniczeniu wielu strat związanych z informacją, niezależnie od tego, gdzie ona istnieje.