NORMY BEZPIECZEŃSTWA PRODUKTÓW

WSTĘP

Organizacje, ludzie, urządzenia, testy, oprogramowanie i produkty mają definiujące cechy. Standardy są ustanawiane w celu zapewnienia jednolitości podstawowych cech między różnymi instancjami takich bytów. Normy pozwalają zatem różnym stronom zrozumieć i porównać definiujące cechy różnych podmiotów. Istnieje wiele rodzajów norm w zależności od charakterystyki, do której się odnoszą. Istnieje również wiele różnych organów lub organów, które opracowują i wydają normy. Szczególnym celem standaryzacji na arenie bezpieczeństwa jest ewolucja w kierunku gospodarki opartej na technologiach informatycznych (IT), w której produkty zabezpieczające i produkty zabezpieczone zbliżają się do stanu plug-and-play. Powinny one cieszyć się porównywalnym zaufaniem, być dostępne do zakupu od wielu konkurencyjnych dostawców oraz umożliwiać mieszanie, dopasowywanie i integrowanie w celu zapewnienia wymaganej bezpiecznej, godnej zaufania infrastruktury informatycznej, która zmniejsza największe ryzyko. W sektorze rządowym Stanów Zjednoczonych bezpieczeństwo produktów i zapewnienie jakości oprogramowania są ważne od lat. Jednak bezpieczeństwo stało się głównym przedmiotem zainteresowania szefów agencji rządowych ds. bezpieczeństwa informacji w wyniku Federalnej Ustawy o Zarządzaniu Bezpieczeństwem Informacji (FISMA).1 FISMA dotyczy bezpieczeństwa systemów. W tym rozdziale nie uwzględniono bezpieczeństwa systemów, takich jak te, na które ma wpływ FISMA i inne normy branżowe mające zastosowanie do bezpiecznych systemów. Ale takie standardy z pewnością zwiększyły uwagę na bezpieczeństwo związane z pojedynczym produktem. Chociaż istnieje kilka różnych kategorii norm związanych z bezpieczeństwem, ten rozdział zawiera wgląd w dziedzinę norm bezpieczeństwa, biorąc pod uwagę tylko reprezentatywną próbkę wielu norm odnoszących się do bezpieczeństwa produktu. Normy związane z budowaniem zaufania do produktów są szczególnie ważne w przeplatanym elektronicznie świecie. W związku z tym główny nacisk położony jest na standardy dotyczące zaufania do produktu.

Wartość norm

Ze standardów związanych z bezpieczeństwem korzysta wiele stron: klienci, dostawcy, twórcy oprogramowania, domy testowe, recenzenci produktów w mediach, konsultanci i nie tylko. Na przykład klienci uważają normy za przydatne na kilka sposobów. Normy pomagają określić ich potrzeby w zakresie różnych funkcji bezpieczeństwa oraz wymagane stopnie pewności w kupowanych produktach. Standardy pomagają klientom zrozumieć, jakie funkcje bezpieczeństwa i gwarancje zapewnia producent produktu. Normy pomagają konsumentom wybrać gotowe produkty komercyjne, co do których mogą mieć pewność, że spełnią ich wymagania w zakresie bezpieczeństwa i gwarancji oraz że w razie potrzeby będą współdziałać z porównywalnymi produktami. Standardy zaopatrzenia pomagają klientom kupować odpowiednio zaufane produkty, które spełniają wymagania klientów. Klienci podlegający przepisom dotyczącym bezpieczeństwa narzuconym przez przepisy federalne, takie jak Ustawa o przenośności i odpowiedzialności w ubezpieczeniach zdrowotnych (HIPAA) oraz Ustawa Sarbanes-Oxley (SOX), często chcą ustanowić należytą staranność, wykorzystując produkty, które cieszą się zaufaniem ich klientów. funkcje bezpieczeństwa i gwarancji w standardowy sposób. Standardowe certyfikaty bezpieczeństwa personelu klienta i zatrudnionych konsultantów pomagają klientom zatrudniać odpowiednio kompetentnych ludzi do ochrony obiektów i informacji klientów lub do pomocy w kontaktach z niektórymi dostawcami lub organami regulacyjnymi. Sprzedawcy i usługodawcy uważają normy za przydatne na kilka sposobów. Korzystanie ze standardów stanowi dowód na to, że dostawcy przenieśli rozwój swoich produktów do paradygmatu, w którym bezpieczeństwo jest wbudowane od samego początku. Korzystanie ze standardów dostarcza dowodów na to, że bezpieczeństwo nie jest kwestią późniejszej refleksji, którą można załatać lub przykręcić.

Stosowanie standardów wdrożeniowych i standardowych certyfikatów personelu pokazuje, że bezpieczeństwo jest fundamentem, na którym sprzedawca buduje produkt lub usługodawca świadczy usługę. Stosowanie standardów pomaga otwierać globalne rynki dla dostawców i usługodawców. Wykorzystując standardową weryfikację funkcji bezpieczeństwa przez stronę trzecią, dostawcy wytwarzają swoje produkty (a usługodawcy wykonują swoje usługi) albo wyróżniać się, albo być porównywalnym do swoich konkurentów. zaufane produkty, które spełniają wymagania klientów. Klienci podlegający przepisom dotyczącym bezpieczeństwa narzuconym przez przepisy federalne, takie jak Ustawa o przenośności i odpowiedzialności w ubezpieczeniach zdrowotnych (HIPAA) oraz Ustawa Sarbanes-Oxley (SOX), często chcą ustanowić należytą staranność, wykorzystując produkty, które cieszą się zaufaniem ich klientów. funkcje bezpieczeństwa i gwarancji w standardowy sposób. Standardowe certyfikaty bezpieczeństwa personelu klienta i zatrudnionych konsultantów pomagają klientom zatrudniać odpowiednio kompetentnych ludzi do ochrony obiektów i informacji klientów lub do pomocy w kontaktach z niektórymi dostawcami lub organami regulacyjnymi.

Sprzedawcy i usługodawcy uważają normy za przydatne na kilka sposobów. Korzystanie ze standardów stanowi dowód na to, że dostawcy przenieśli rozwój swoich produktów do paradygmatu, w którym bezpieczeństwo jest wbudowane od samego początku. Korzystanie ze standardów dostarcza dowodów na to, że bezpieczeństwo nie jest kwestią późniejszej refleksji, którą można załatać lub przykręcić. Stosowanie standardów wdrożeniowych i standardowych certyfikatów personelu pokazuje, że bezpieczeństwo jest fundamentem, na którym sprzedawca buduje produkt lub usługodawca świadczy usługę. Stosowanie standardów pomaga otwierać globalne rynki dla dostawców i usługodawców. Stosując standardową weryfikację zabezpieczeń przez stronę trzecią, dostawcy sprawiają, że ich produkty (a usługodawcy świadczą usługi) wyróżniają się na tle konkurencji lub są z nią porównywalne. Motywacja do budowania zaufania i zarządzania ryzykiem w produktach.

Zaufanie do elektronicznego przetwarzania, przechowywania i interakcji między klientami, firmami, partnerami biznesowymi, dostawcami, organizacjami usługowymi i rządami jest kluczem do elektronicznych modeli gospodarki, elektronicznej opieki zdrowotnej i elektronicznych rządów. Potrzeba zaufania będzie tylko rosła w miarę rozprzestrzeniania się nowych paradygmatów i technologii informatycznych, mutacji modeli biznesowych i modeli wsparcia IT oraz wprowadzania nowych zagrożeń i słabych punktów. Aby modele usług elektronicznych odniosły sukces, wszyscy uczestnicy e-biznesu, e-zdrowia i e-administracji muszą mieć zaufanie do produktów IT używanych przez graczy wchodzących w interakcje, jak również do produktów używanych w interweniującej infrastrukturze IT. Innym kluczowym pojęciem poza zaufaniem jest pojęcie zarządzania ryzykiem. Kiedy między stronami ustanawiane są relacje elektroniczne, istnieje wymierne ryzyko związane z takimi relacjami. Ryzyko można zmierzyć na wiele sposobów. Na przykład można je określić ilościowo pod względem rodzajów możliwych zdarzeń niepożądanych. Można je skwantyfikować pod względem prawdopodobieństwa wystąpienia różnego rodzaju zdarzeń niepożądanych oraz wartości tego, co ma być chronione przez rozwiązania bezpieczeństwa IT podczas zdarzenia niepożądanego. Można je określić ilościowo pod kątem skutków zdarzeń niepożądanych, takich jak odpowiedzialność, która może zostać narażona na kompromisy lub podmioty, które mogą zostać poszkodowane przez kompromisy. Ryzyka można zatem łagodzić na wiele możliwych sposobów. Na przykład ryzyko można ograniczyć, stosując produkty, które ograniczają występowanie lub skutki zdarzeń niepożądanych budzących największe obawy. Gdy aktywa o rosnącej wartości wymagają ochrony, ryzyko można zmniejszyć, stosując produkty o zwiększonej pewności. Ryzyko można również złagodzić, stosując produkty, które zmniejszają określone, szkodliwe zobowiązania i niepożądane konsekwencje budzące największe obawy. Możliwość określenia budzących obawy zagrożeń i zidentyfikowania rozwiązań bezpieczeństwa, które je ograniczają, jest potężną strategią stosowaną w ramach niektórych podejść opartych na standardach, takich jak paradygmat Common Criteria (CC). Połączenie pojęcia zaufania z

pojęciem redukcji ryzyka tworzy potężną strategię. Budowanie zaufania między współpracującymi stronami elektronicznymi, że wszystkie strony używają produktów o odpowiedniej jakości zabezpieczeń, jest podobne do roli uścisków dłoni twarzą w twarz w starszych modelach biznesowych. Na rynku e-biznesu zaufanie, podobnie jak stare zasady, jest kluczem do zwiększenia przychodów poprzez zwiększenie wolumenu transakcji biznesowych. Ponadto, ograniczając ryzyko, można ograniczyć straty biznesowe i koszty. Kiedy wzmacnianie zaufania jest połączone z zarządzaniem ryzykiem, wynikające z tego zwiększone przychody, w połączeniu ze zmniejszonymi stratami i niższymi kosztami, przyczyniają się do znacznego zwielokrotnienia zysków. Paradygmat CC jest przykładem strategii oceny produktów opartej na standardach, która zapewnia zarówno ustanowienie odpowiedniego poziomu zaufania do produktów, jak i określanie, zarządzanie i łagodzenie ryzyka budzącego największe obawy. Na przestrzeni lat opracowano i wykorzystano różne oparte na standardach sposoby budowania zaufania co do jakości implementacji zabezpieczeń. Działania takie koncentrują się na budowaniu zaufania z jednej lub obu z dwóch perspektyw: (1) że produkt pełni deklarowane funkcje bezpieczeństwa całkowicie i poprawnie oraz (2) że procesy konstruktora produktu (od projektu, przez rozwój, po dostawę, konserwacja) są prawidłowe. Zwykle zaufanie buduje się albo poprzez standardowe testowanie samej implementacji, albo poprzez standardową ocenę zarówno produktu, jak i jego wdrażającego. Nie wszystkie podejścia do budowania zaufania poprzez ocenę produktu muszą odnosić się do zaufania poprzez formalną, opartą na standardach ocenę wdrożonych funkcji bezpieczeństwa, jak również zapewnienie solidności zdolności i procesów konstruktora. Oznacza to, że wiele podejść do testowania i oceny opiera się na standardach nieformalnych, de facto lub de iure2, a nie na formalnych, uznanych na szczeblu krajowym standardach.

Motywacja do budowania zaufania do systemów

Niedawne administracje rządowe Stanów Zjednoczonych uznały znaczenie budowania zaufania do technologii informatycznych. Wydały dyrektywy i wytyczne mające na celu podniesienie świadomości na temat centralnego, krytycznego charakteru IT oraz pomoc w utrzymaniu zaufania do krajowych infrastruktur IT. Krajowe infrastruktury informatyczne to zazwyczaj duże systemy informatyczne, często składające się z wielu pojedynczych produktów. Oparte na standardach metody budowania zaufania do produktów niekoniecznie sprawdzają się w budowaniu zaufania do systemów. Istnieją oparte na standardach metody budowania zaufania do systemów informatycznych. Obejmują one na przykład standardy i działania testowe związane z pierwotnym procesem certyfikacji i akredytacji technologii informatycznych Departamentu Obrony Stanów Zjednoczonych (DITSCAP)3 oraz Proces certyfikacji i akredytacji Departamentu Obrony w zakresie zapewniania informacji (DIACAP)4, który go zastąpił, FISMA rządu Stanów Zjednoczonych oraz standard bezpieczeństwa danych branży kart płatniczych (PCI DSS) społeczności finansowej. Takie skoncentrowane na systemach metody budowania zaufania są zwykle stosowane tylko przez duże przedsiębiorstwa. Ponadto ewoluuje problem ustalenia ilościowej miary zaufania do bardzo dużego, heterogenicznego systemu, jakim jest krajowa infrastruktura informatyczna. Wymaga co najmniej koordynacji i współpracy między wszystkimi, którzy wnoszą wkład w infrastrukturę lub z niej korzystają. Wymogi bezpieczeństwa i podejścia do testowania bezpieczeństwa mające zastosowanie do systemów informatycznych jako takich nie są tutaj brane pod uwagę. Chociaż wśród specjalistów ds. bezpieczeństwa nadal trwają spory, wielu uważa, że krokiem we właściwym kierunku jest budowanie systemów informatycznych z produktami i komponentami, które są indywidualnie oceniane jako godne zaufania, z pewnym określonym stopniem zaufania. Jednak najtrudniejsze w ocenie produktu jest przetestowanie aspektów bezpieczeństwa produktu w środowisku, które doskonale naśladuje środowisko, w którym produkt ma być używany.

RODZAJE, ŹRÓDŁA I PRZYKŁADY NORM

W dzisiejszych heterogenicznych, multidyscyplinarnych, wielotechnologicznych, wielostronnych, wzajemnie połączonych środowiskach IT różne rodzaje standardów bezpieczeństwa są niezbędne z różnych powodów. Kilka formalnych, nieformalnych i ad hoc organów opracowuje i wydaje standardy. Znaczenie i akceptacja danego standardu zwykle zależy od rozgłosu organu, który ten standard tworzy.

Rodzaje norm

W świecie bezpieczeństwa istnieje wiele różnych rodzajów standardów. Rodzaje norm związanych z bezpieczeństwem obejmują następujące:

* Standardy zdolności

* Certyfikaty personelu

* Kryteria oceny ryzyka

* Specyfikacje wymagań

* Specyfikacje funkcjonalne

* Specyfikacje ubezpieczenia

* Kryteria wydajności

* Standardy rozwoju produktu

* Testowanie, ocena i standardy/kryteria oceny6

* Kryteria oceny produktu

* Standardy interoperacyjności

* Standardy zamówień

* Normy pomocnicze

Źródła norm

Oto niektóre z organów, które wydają formalne, uznane przez narody standardy, standardy organizacyjne lub zastrzeżone standardy, lub które stosują podejście de iure związane z bezpieczeństwem:

* Uznane organy krajowe

* Organizacje międzynarodowe

* Rządy

* Wojskowy

* Konsorcja

* Podobnie myślące społeczności

* Sprzedawcy

* Domy konsultingowe

* Prasa branżowa

* Komercyjne domy testowe

* Prywatni wykonawcy testów

Formalne standardy dotyczące zapewniania informacji (IA) są tworzone, publikowane i utrzymywane przez uznane organy normalizacyjne. Istnieją różne uznane organy normalizacyjne, w tym grupy robocze zajmujące się specyficzną technologią, stowarzyszone z organizacjami zawodowymi, takimi jak IEEE (Instytut Inżynierów Elektryków i Elektroników) oraz IETF (Internet Engineering Task Force). Normy są również tworzone przez grupy robocze zrzeszone w uznanych, właściwych dla danego kraju, krajowych organach normalizacyjnych, takich jak np. ASC (American Standards Committee, dawniej ANSI) w Stanach Zjednoczonych, BSI (British Standards Institute) w Wielkiej Brytanii oraz Bundesamt für Sicherheit in der Informationstechnik (również BSI) w Niemczech. Takie krajowe organy normalizacyjne tworzą albo normy dla poszczególnych krajów, albo współpracują i harmonizują z innymi równorzędnymi krajowymi organami normalizacyjnymi w celu stworzenia międzynarodowych, obowiązujących na całym świecie norm, takich jak te związane z Międzynarodową Organizacją Normalizacyjną (ISO). Uznane organizacje w ramach rządów krajowych również tworzą standardy. Na przykład National Institute of Standards and Technology (NIST) — amerykańska agencja federalna podlegająca Departamentowi Handlu Stanów Zjednoczonych — tworzy i wydaje standardy zwane Federalnymi Standardami Przetwarzania Informacji (FIPS). Wydaje również standardy zwane SP (publikacje specjalne), które określają wytyczne dotyczące najlepszych praktyk w zakresie bezpieczeństwa, prywatności i pewności. FIPS i SP często mają zastosowanie nie tylko do rządu Stanów Zjednoczonych, ale są szeroko stosowane jako referencje w innych organizacjach pozarządowych, a niektóre mogą nawet formalnie obowiązywać. Na przykład poprawka z 2005 r. do Federal Acquisition Regulation, mająca na celu wdrożenie przepisów FISMA dotyczących bezpieczeństwa IT, wymaga, aby wszystkie zamówienia federalne były zgodne z odpowiednimi normami i publikacjami NIST. Rządy krajowe tworzą również organy do współpracy i harmonizacji międzynarodowych standardów do użytku przez rządy w kilku krajach. Projekt CC jest przykładem takiego międzyrządowego organu normalizacyjnego. Normy opracowane przez ten konkretny międzyrządowy organ normalizacyjny są również przekazywane uznanym międzynarodowym organom normalizacyjnym, takim jak ISO, w celu stworzenia norm o jeszcze szerszym zasięgu. W obszarze wojskowym Departament Obrony USA publikuje standardowe dyrektywy wojskowe, takie jak Mil Standard 8500,8,9, których należy przestrzegać przy zakupie produktów związanych z bezpieczeństwem, a także dyrektywę Departamentu Obrony 857010, która dotyczy szkolenia, certyfikacji i zarządzania pracownicy pełniący funkcje IW. Konsorcja zajmujące się specyficzną technologią i branżą mają duże, szeroko zakrojone, międzynarodowe członkostwo; Przykłady obejmują

* Cloud Security Alliance (CSA)

* Security Standards Council (SSC) konsorcjum Payment Card Industry (PCI).

* Forum Software Assurance na rzecz doskonałości w kodzie (SAFECode)

* Grupa zarządzania obiektami (OMG)

* Konsorcjum ds. bezpieczeństwa aplikacji internetowych (WASC)

* Forum TM (dawniej TeleZarządzanie).

Często uważa się ich za twórców nieformalnych standardów związanych z bezpieczeństwem do użytku w określonych branżach lub sektorach technologicznych. Małe konsorcja lub pojedyncze podmioty

również twierdzą, że tworzą standardy, ale takie wysiłki generalnie nie są akceptowane przez tak szerokie grupy odbiorców, jak legalne, uznane, formalne i nieformalne standardy. Inne podobnie myślące społeczności, takie jak SANS (dawniej System Administration and Network Security) Institute, ogłaszają de facto najlepsze praktyki w zakresie standardów bezpieczeństwa, takie jak 20 Critical Controls, które twierdzą, że odzwierciedlają konsensus społeczności w ramach pewnej społeczności praktyków bezpieczeństwa. Dostawcy, tacy jak Microsoft, opracowują dokumenty podobne do standardów, takie jak PCI DSS Compliance Planning Guide lub ramy cyklu życia bezpiecznego programowania i strategię bezpiecznego kodowania, które prawdopodobnie mają nadzieję, że zostaną przyjęte przez duże społeczności. Domy konsultingowe, takie jak Gartner, Forrester i Frost & Sullivan, opracowują prywatne kryteria przeglądu produktów dotyczące zabezpieczeń i funkcji zabezpieczających. Stosują takie kryteria do oceny produktów związanych z bezpieczeństwem. Gartner i inni również opracowują recenzje produktów na podstawie wywiadów z użytkownikami. Prasa branżowa obejmuje media, takie jak Computerworld, CSO, IT Business Edge, Network World, SC Magazine i Security Management, które tworzą jeszcze inne prywatne kryteria przeglądu produktów, których używają do badania produktów związanych z bezpieczeństwem. Komercyjne domy testujące, takie jak ICSA Labs, NSS Labs i West Coast Labs, tworzą i wykorzystują prywatne, niezależne kryteria i metodologie testowania produktów do oceny bezpieczeństwa i wydajności produktów. Niektóre komercyjne domy testujące, takie jak AV-Test, opracowują prywatne, niezależne kryteria testowania produktów i metody certyfikacji testowanych produktów. Prywatni kontrahenci przeprowadzają testy bezpieczeństwa produktów za pomocą różnych nieformalnie standardowych technik, które opierają się na prywatnych kryteriach i procedurach testowych. Takie techniki obejmują skanowanie podatności na zagrożenia, ocenę podatności na zagrożenia, testy penetracyjne, audyty bezpieczeństwa, audyty ISO 27001, przeglądy bezpieczeństwa, hakowanie etyczne i inne. Organizacje akademickie również zaczynają tworzyć laboratoria oceny produktów zabezpieczających, które opierają się na różnych opublikowanych procedurach i kryteriach testów podatności i pewności.

Przykłady standardów bezpieczeństwa. Przykłady rodzajów norm dotyczących bezpieczeństwa wydanych przez różne organy wydające normy przedstawiono w tej sekcji poniżej. Szczegółowe streszczenia niektórych z tych standardów znajdują się w dalszej części tego rozdziału. Standardy zdolności, takie jak Capability Maturity Model (CMM) i ISO 9000, służą do mierzenia kompetencji organizacji, które tworzą produkty - w szczególności produkty związane z bezpieczeństwem. Ogólne certyfikaty personelu, takie jak Certified Information Systems Security Professional (CISSP) z Międzynarodowego Konsorcjum Certyfikacji Bezpieczeństwa Systemów Informatycznych (ISC)2, mierzą między innymi kompetencje personelu w określaniu, budowaniu, zamawianiu, instalowaniu lub utrzymywaniu bezpieczeństwa Produkty powiązane. Inne certyfikaty, takie jak IEEE Computer Society's Certified Software Development Associate (lub Professional) lub (ISC)2 Certified Secure Software Lifecycle Professional (CSSLP) lub Electronic Commerce Council Certified Secure Programmer to przykłady certyfikatów bardziej bezpośrednio przydatnych w niektórych obszarach rozwoju oprogramowania produktowego z udziałem bezpieczeństwa. Certyfikat Cloud Security Alliance wydany przez Cloud Security Alliance ocenia kompetencje danej osoby w głównych kwestiach związanych z bezpieczeństwem w chmurze. Istnieją normy zapewniające spójne sposoby określania potrzeb i wymagań w zakresie bezpieczeństwa zarówno w przypadku produktów zabezpieczających, jak i produktów zabezpieczonych. Niektóre normy określają funkcje bezpieczeństwa pojawiające się w produktach. Standardy, takie jak IETF IPSec, nie tylko określają funkcje bezpieczeństwa, ale także wspierają interoperacyjność oddzielnie budowanych implementacji zabezpieczeń. Inne standardy określają interfejsy oprogramowania związane z bezpieczeństwem, konwencje nazewnictwa i struktury danych, takie jak produkty oprogramowania pośredniego Common Object Request Broker Architecture (CORBA). Standardy, takie jak FIPS 140, mogą określać wymagania bezpieczeństwa,

metody oceny i koncepcje sprawdzania poprawności dla pojedynczego określonego typu składnika lub produktu związanego z bezpieczeństwem. Normy z serii CC mogą określać funkcje bezpieczeństwa i charakterystykę zapewniania bezpieczeństwa, które mają być włączone do dowolnej klasy produktów. Normy de iure, takie jak SANS 20 Critical Controls, które konkurują z niektórymi normami krajowymi i międzynarodowymi, określają pojedynczy, mały, podstawowy rdzeń funkcji bezpieczeństwa. Ten de iure, oparty na konsensusie standard może zyskiwać na popularności. Normy rozwoju produktów, takie jak ISO/IEC 27034-1, określają wymagania dotyczące bezpiecznych procesów tworzenia oprogramowania, podczas gdy standard branżowy Building Security in Maturity Model (BSIMM) de facto zapewnia możliwość porównywania bezpiecznych środowisk kodowania i identyfikowania najlepszych praktyk programistycznych. Standardy dostawców, takie jak Security Development Lifecycle firmy Microsoft, określają również procesy tworzenia i zapewniania oprogramowania w celu zwiększenia niezawodności zabezpieczeń oprogramowania. Istnieją również normy regulujące testowanie produktów. Istotne jest, aby sprzedawcy i nabywcy produktów zabezpieczających i produktów o ulepszonych zabezpieczeniach (a) weryfikowali, czy testowany produkt implementuje funkcjonalność spełniającą określone wymagania funkcjonalne dotyczące bezpieczeństwa oraz (b) wykazali, w jakim stopniu produkt i procesy rozwoju produktu dostawcy spełniają określone wymagania. Istnieją krajowe i międzynarodowe standardy, takie jak FIPS 140 i CC, które określają takie testy zgodności i określają metody testowania w celu przeprowadzenia takich testów. Standardowe podejście FedRAMP dotyczy walidacji możliwości bezpieczeństwa związanych z określoną klasą dostawców usług. Zgodność różnych produktów związanych z bezpieczeństwem z tym samym standardem funkcjonalnym niekoniecznie gwarantuje jednak, że produkty te będą współdziałać. Interoperacyjność oddzielnie produkowanych rozwiązań bezpieczeństwa jest możliwa, jeśli standardy implementacyjne mogą określać precyzyjne, interoperacyjne profile wybranych możliwości bezpieczeństwa w ramach standardu funkcjonalnego bezpieczeństwa. Testy interoperacyjności mogą zapewnić bezpieczną współpracę między porównywalnymi produktami tworzonymi przez niezależnych dostawców i używanymi przez niezależne podmioty. Zgodność oznacza jedynie, że interoperacyjność jest możliwa; ale interoperacyjność należy zweryfikować za pomocą testów parami. Standardy istnieją po to, aby określić, jak badać zgodność wdrożeń ze standardami funkcjonalnymi i jak zapewnić interoperacyjność wdrożeń, które muszą spełniać ten sam standard funkcjonalny. Nie można ufać współpracującym, zgodnym, zabezpieczonym produktom i produktom zabezpieczającym, że zapewniają lub wspierają należyte bezpieczeństwo lub ograniczają największe zagrożenia. Kluczem do budowania zaufania jest zbudowanie pewności, że produkty ograniczają potencjalne ryzyko, że produkty są odpowiednio zbudowane i zachowują się zgodnie ze specyfikacją oraz że produkty nie działają więcej ani nie mniej niż reklamowane. Istnieją standardy, takie jak CC, służące do ustalania i testowania stopnia, w jakim ryzyko i luki w zabezpieczeniach są ograniczane do określonego poziomu ufności. Normy te określają wymagania dotyczące zapewnienia bezpieczeństwa implementacji oraz związane z nimi testy i metody testowania w celu weryfikacji jakości wdrożonych zabezpieczeń w ramach testowanych produktów. Jeśli chodzi o prywatne standardy de iure, różne branżowe media prasowe i inne opracowują prywatne kryteria i metodologie przeglądu produktów. Te prywatne standardy są wykorzystywane do tworzenia recenzji określonych produktów zabezpieczających lub produktów o zwiększonym poziomie bezpieczeństwa lub do opracowywania przewodników dla kupujących, które porównują indywidualne recenzje kilku produktów w ramach danej klasy produktów. Pewne metryki tworzone na podstawie takich kryteriów mogą dostarczać miar wydajności zabezpieczeń. Niektóre media prowadzą programy nagród, które wykorzystują ankiety oparte na pytaniach w celu identyfikacji wybranych przez czytelników najlepszych produktów w określonych klasach produktów. Istnieją również nagrody za przywództwo produktowe oparte na popularności. W obszarze standardów zamówień, normy takie jak DoD 8500.1 i 8500.2 określają odpowiednio standardowe zasady polityki i dyrektywy w sprawie wdrażania polityki, dla jakich rodzajów produktów

musi zamawiać Departament Obrony. Normy te określają również, co muszą zrobić jednostki Departamentu Obrony, aby zaspokoić potrzebę lub jakie ograniczenia organizacje Departamentu Obrony muszą przestrzegać przy zamawianiu produktów IT. W obszarze standardów pomocniczych, standardy takie jak standardy towarzyszące w ramach pakietu standardów CC określają, jak zostać testerem produktów i jak akredytować organizacje do przeprowadzania testów zgodności, zaufania lub interoperacyjności w standardowy sposób. Inne standardy pomocnicze – nieuwzględnione w tym rozdziale – takie jak DITSCAP21 (zastąpiony przez DIACAP w listopadzie 2007) dla Departamentu Obrony Stanów Zjednoczonych, National Information Assurance Certification and Accreditation Process (NIACAP)22 oraz NIST Certification & Accreditation (C&A)23 metodologie dla Federalne departamenty i agencje cywilne USA określają, jak certyfikować i jak akredytować systemy składające się z bezpiecznych produktów i bezpiecznych komponentów. Normy takie jak ISO 1779924 i NIST SP 800-5325 mogą określać wytyczne lub najlepsze praktyki dla użytkowników montujących i korzystających z bezpiecznych komponentów. Ogólnie rzecz biorąc, standardy promują spójne bezpieczeństwo, od początku do końca, jak również w różnych domenach publicznych i prywatnych oraz środowiskach komputerowych.

PODEJŚCIA DO ROZWOJU I OCENY PRODUKTÓW

Ten rozdział koncentruje się na standardach zwiększania zaufania do produktów związanych z bezpieczeństwem. Istnieją dwie klasy produktów będących przedmiotem zainteresowania: produkty „zabezpieczające" i produkty „z włączonymi zabezpieczeniami". Produkty zabezpieczające bezpośrednio zapewniają usługi bezpieczeństwa lub zapobiegają penetracji. Produkty zabezpieczające obejmują na przykład produkty do wykrywania włamań i zapory sieciowe. Produkty z zabezpieczeniami to produkty zabezpieczone, które nie służą wyłącznie do świadczenia usług bezpieczeństwa; zamiast tego świadczą inne usługi, które są chronione. Przykłady obejmują systemy operacyjne, systemy zarządzania bazami danych i wirtualne sieci prywatne, które zawierają funkcje bezpieczeństwa, takie jak identyfikacja i uwierzytelnianie lub IPSec w celu ochrony produktu lub usług świadczonych przez produkt. Pozostała część tego rozdziału podsumowuje różne podejścia, które wspierają wzrost zaufania do takich produktów. Rząd Stanów Zjednoczonych miał nadzieję, że wszyscy konsumenci, sprzedawcy i testerzy produktów związanych z bezpieczeństwem z sektora publicznego i prywatnego skupią się wokół formalnych, uznanych na całym świecie standardów dotyczących specyfikacji, rozwoju, testowania i oceny takich produktów. Ponieważ normy formalne były opracowywane przez krajowe i międzynarodowe organy normalizacyjne, oczekiwano, że konsumenci będą mogli z większą pewnością zrozumieć zabezpieczenia i zabezpieczenia oferowane przez produkt lub usługodawcę. Oczekiwano, że zaufanie uzyskane dzięki zastosowaniu uniwersalnych, akceptowanych na całym świecie standardów będzie ostro kontrastować z niestandardowymi podejściami, które ze względu na samą liczbę konkurencyjnych podejść będą konfrontować i dezorientować konsumentów. W dzisiejszych czasach sektory rządowy i wojskowy często opierają się na podejściach opartych na formalnych standardach. Ale z drugiej strony — pomimo oczekiwań związanych z takim formalnym podejściem opartym na standardach — cały rynek niekoniecznie zjednoczył się wokół formalnego podejścia do standardów. Powstało wiele nieformalnych, prywatnych alternatyw oceny produktów, które nie opierają się na formalnych standardach i są stosowane z większą lub mniejszą częstotliwością niż alternatywy oparte na formalnych standardach. Nie brakuje alternatywnych podejść i alternatywnych ram, na których opierają się takie podejścia. Odpowiednio, nie brakuje podejść określonych w dyrektywach dotyczących zamówień użytkowników. Rynek jest podzielony na wiele alternatyw. Poniżej przeanalizowano próbkę tych alternatyw.

Historyczne podejście o zachodzie słońca

Aby wprowadzić spójność w opisywaniu funkcji zabezpieczeń i poziomów zaufania ograniczonego zestawu produktów o podwyższonych zabezpieczeniach oraz ułatwić kompleksowe testowanie i ocenę takich produktów, Departament Obrony Stanów Zjednoczonych opracował kryteria oceny zaufanego systemu komputerowego (TCSEC). TCSEC — często nazywany pomarańczową księgą — zdefiniował niewielki zestaw klas (od C1 do A1) zwiększających funkcjonalność zabezpieczeń i zwiększających pewność, mających zastosowanie do systemów operacyjnych. TCSEC został rozszerzony na urządzenia sieciowe i systemy zarządzania bazami danych. Najpierw zaoferowano rządowe oceny wewnętrzne, a następnie porównywalne komercyjne usługi oceny sponsorowane przez rząd. Częściowo z powodu dużych opóźnień i kosztów testowania, inne kraje opracowały inne kryteria, które były bardziej elastyczne i można je dostosować, aby uwzględnić szybko rozwijające się technologie informatyczne. Kryteria oceny bezpieczeństwa technologii informacyjnej29 (ITSEC) powstały z połączonych danych wejściowych wcześniejszych kryteriów niemieckich, kryteriów francuskich i brytyjskich poziomów zaufania. Następnie opracowano kanadyjskie kryteria oceny zaufanych produktów komputerowych (CTCPEC) jako połączenie podejść TCSEC i ITSEC. Rozwój US Federal Criteria następnie próbował połączyć CTCPEC i ITSEC z TCSEC. Wraz z rozwojem międzynarodowego rynku zaufanych produktów IT wszystkie te historyczne, konkurujące ze sobą kryteria krajowe mogły potencjalnie doprowadzić do pęknięcia rynku. Zostały one wygaszone po zakończeniu wysiłków zmierzających do zharmonizowania różnych kryteriów w celu uzyskania wspólnych, opartych na standardach, akceptowanych na szczeblu międzynarodowym kryteriów. Wynikiem wysiłków harmonizacyjnych był jeden, szeroko zakrojony program CC (sekcja 51.5.3). Te standardowe kryteria zapewniają w pełni elastyczne, wysoce dostosowywalne podejście do standaryzacji funkcji bezpieczeństwa, wymagań dotyczących oceny, specyfikacji i testowania wdrożeń produktów związanych z bezpieczeństwem

Instytut SANS

Instytut SANS wydał normę de iure, która określa podstawowy zestaw najbardziej krytycznych, podstawowych środków kontroli bezpieczeństwa, które są uważane za niezbędne dla praktycznie każdej organizacji. Te kontrole bezpieczeństwa są potocznie nazywane 20 krytycznymi kontrolami. Zapewniają wykonalne, możliwe do wdrożenia, oparte na najlepszych praktykach podejście do bezpieczeństwa oparte na rzekomej największej redukcji ryzyka, najlepszej ochronie przed rzeczywistymi zagrożeniami w terenie oraz najlepszych technikach powstrzymywania najbardziej niebezpiecznych, częste, regularnie występujące ataki. Podejście SANS zapewnia ciągłe, zautomatyzowane monitorowanie kluczowych części infrastruktury IT organizacji w celu zapewnienia skuteczności bezpieczeństwa. Firma SANS opublikowała wytyczne dotyczące sposobu wdrożenia tych krytycznych kontroli. Wytyczne zawierają tabelaryczne zestawienie wielu rzeczywistych ataków i zapewniają mapowanie, które określa, która z 20 kontroli krytycznych zapewnia najlepszą obronę przed każdym z tych ataków. SANS Critical Controls odwzorowuje pewien podzbiór kontroli bezpieczeństwa określonych w publikacji specjalnej NIST 800-53, wersja 3 (patrz Załącznik A wytycznych SANS Critical Controls). W pewnym sensie krytyczne kontrole SANS można uznać za specyficzny profil najważniejszych kontroli bezpieczeństwa w NIST SP 800-53. Niektórzy specjaliści ds. bezpieczeństwa uważają, że kontrola krytyczna SANS 20 zapewni niezbędną (ale niekoniecznie wystarczającą) należytą staranność, aby stać się de facto miarą standardu dbałości o bezpieczeństwo.

Cloud Security Alliance (CSA)

CSA opracowała wytyczne wyjaśniające przetwarzanie w chmurze i identyfikujące najlepsze praktyki oparte na ryzyku dotyczące przejścia do bezpiecznych operacji w chmurze zapewnianych przez różne modele usług w chmurze w środowiskach przetwarzania w chmurze. Podział odpowiedzialności za bezpieczeństwo między klientów chmury i dostawców usług w chmurze zależy od oferowanej usługi w chmurze, na przykład oprogramowanie w chmurze jako usługa (SaaS), infrastruktura chmury jako

usługa (IaaS), platforma chmury jako usługa (PaaS). Określone środki kontroli bezpieczeństwa i technologie mają zastosowanie do (a) ochrony danych migrujących do chmur, (b) ochrony danych przesyłanych do chmury i przesyłanych między różnymi dostawcami chmury/środowiskami chmury, (c) ochrony danych w chmurach, (d) prywatności konserwacja, (e) bezpieczeństwo aplikacji, (f) zapobieganie utracie danych i nie tylko. W chwili pisania tego tekstu (lipiec 2013 r.) dostępna jest wersja 3. wydania niniejszych wytycznych.

Standardowe metody opracowywania produktów

Kluczem, który może prowadzić do produktywnej oceny produktu, jest poleganie przez konstruktorów produktów na wysokiej jakości, wysoce zdolnych programistach produktów oraz stosowanie standardów rozwoju produktu, takich jak standardy projektowania i testowania oprogramowania, podczas projektowania i tworzenia produktu. Takie standardy dotyczące zdolności programistów, które mogą mieć zastosowanie do twórców produktów zabezpieczających, obejmują model dojrzałości zdolności oraz serię norm ISO 9000.

Model dojrzałości zdolności

Systems Security Engineering Capability Maturity Model (SSE-CMM) został znormalizowany jako ISO/IEC 21827. Norma ta zapewnia sposób oceny solidności praktyk inżynieryjnych konstruktora produktów bezpieczeństwa, a także sposób ciągłego doskonalenia tych praktyk w górę hierarchia coraz bardziej dojrzałych poziomów procesu tworzenia oprogramowania na wielu etapach rozwoju produktu, takich jak:

* Wychwytywanie i analiza wymagań produktowych

* Definicja koncepcji produktu, w tym dokładne przełożenie wymagań bezpieczeństwa na wymagania produktu

* Architektura produktu

* Projekt produktu

* Wdrożenie produktu

Twórca produktu zabezpieczającego może wykazać się kompetencjami w budowaniu produktów za pomocą uznanych, tak zwanych ocen dojrzałości zdolności oprogramowania dewelopera i procesów inżynierii bezpieczeństwa. Produkty o zwiększonym poziomie bezpieczeństwa tworzone przez organizacje o udokumentowanej wiedzy i dojrzałości mogą zasługiwać na większe zaufanie niż produkty tworzone przez organizacje, które nie wykazują dojrzałych, kompetentnych możliwości w zakresie projektowania oprogramowania i inżynierii bezpieczeństwa. SSE-CMM ustanawia ramy ogólnie przyjętych zasad inżynierii bezpieczeństwa oraz standardowy sposób mierzenia (i ulepszania) skuteczności praktyk inżynierii bezpieczeństwa organizacji. SSE-CMM opisuje podstawowe cechy i zapewnia narzędzia do oceny procesu inżynierii bezpieczeństwa w organizacji, który musi istnieć, aby zapewnić dobrą inżynierię bezpieczeństwa. Cechy te są oceniane za pomocą zestawu metryk bezpieczeństwa, które oceniają określone atrybuty dotyczące procesów dostawcy oraz skuteczność bezpieczeństwa wyników procesów dostawcy. Kiedy poziom metryk bezpieczeństwa SSE-CMM powiązany z konkretnym konstruktorem pokazuje, że konstruktor ma dojrzałe możliwości inżynierii bezpieczeństwa i skuteczne praktyki inżynierii bezpieczeństwa, wtedy wzrasta pewność, że konstruktor może zbudować solidne produkty bezpieczeństwa. Zaufanie i pewność co do produktu można do pewnego stopnia wywnioskować w przypadku wymiernie kompetentnych dostawców, którzy stosują solidne procesy inżynierii bezpieczeństwa, zgodnie z oceną SSE-CMM. Ilościowa porównywalność

pewności uzyskana dzięki podejściu SSECMM z pewnością uzyskaną za pomocą innych podejść, takich jak ocena wymogów dotyczących pewności określonych w paradygmacie CC, nie jest dobrze poznana. Na razie wydaje się, że możliwa jest ocena pewności co do zdolności dostawcy do tworzenia produktów wysokiej jakości zarówno za pomocą podejścia SSE-CMM, jak i CC; ale być może oba podejścia powinny zostać zintegrowane, aby stworzyć bardziej kompleksowy model oceny pewności.

Normy ISO 9000. Norma ISO 900033 jest stosowana jako przewodnik do przeprowadzania szerokiej, horyzontalnej oceny jakości systemów i kompetencji organizacji (zwykle organizacji produkcyjnej lub usługowej) we wszystkich jej aspektach. Chociaż nie jest specyficzna dla organizacji tworzących produkty zabezpieczające, dostarcza pewnych podstawowych informacji o potencjale jakości i powtarzalności zdolności organizacji do wypełnienia swojej misji. W rzeczywistości normy pochodne, takie jak w CC, częściowo inspirowane ISO 9000, są wykorzystywane do akredytacji jakości związanej z laboratoriami testującymi bezpieczeństwo. Norma ISO 9001 ma zastosowanie do tworzenia oprogramowania. Chociaż nie jest specyficzna dla organizacji tworzących produkty zabezpieczające, to jednak ogólnie określa akceptowalny, minimalny poziom jakości dla procesów oprogramowania.

Standardy i podejścia do opracowywania produktów

Istnieje wielka potrzeba skupienia się na bezpiecznym rozwoju oprogramowania, ponieważ nowe produkty są wprowadzane na rynek. Obecna sytuacja w zakresie tworzenia bezpiecznego oprogramowania nie jest najlepsza. Rocznie wykrywanych jest około 5000 nowych luk w oprogramowaniu — wiele z nich można wykorzystać w rzeczywistych zagrożeniach i atakach. Niestety, sabotaż oprogramowania obejmuje również zamierzone, złowrogie wady. Badania wskazują, że nawet 99 procent zaszyfrowanych aplikacji zawiera luki w zabezpieczeniach. Sterowanie przemysłowe, tak zwane oprogramowanie do kontroli nadzorczej i akwizycji danych (SCADA), jest równie podatne na ataki. Rzeczywiście, choć nieco lepsze niż te statystyki dla ogólnych zastosowań, nawet oprogramowanie w urządzeniach zabezpieczających nie jest odporne na wady programistyczne i nie jest – jak wielu klientów może sądzić – z natury bezpieczne. Aby przezwyciężyć zagrożenia dla oprogramowania, naukowcy zajmujący się oprogramowaniem zabezpieczającym próbują przenieść praktyki tworzenia bezpiecznego oprogramowania ze sztuki do nauki opartej na standardach. Typowe strategie łagodzenia skutków obejmują ustanowienie odpowiednich i raczej konkretnych zasad i procedur (które powinny obejmować przykłady kodowania) w celu zarządzania bezpiecznym rozwojem oprogramowania. Specyficzne taktyki obejmują na przykład poleganie na powszechnie dostępnych, standardowych technologiach zorientowanych na zachowanie równowagi, takich jak

* Podpisywanie kodu przez programistów,

* Monitory kontroli sprawdzania kodu i ścieżki audytu,

* Wielostronne, wzajemnie monitorujące się przeglądy kodu,

* Automatyczne skanowanie kodu i luk w zabezpieczeniach z akceptowalnymi współczynnikami wykrywania fałszywie dodatnich/negatywnych wyników,

* Skanowanie ataków na żywo i

* Wykorzystanie technologii antysabotażowej do sprawdzania integralności kodu.

Istnieją wytyczne dotyczące bezpiecznego tworzenia oprogramowania.35,36 Komercyjne narzędzia do testowania rozwoju, takie jak statyczne i dynamiczne analizatory kodu, mogą być również wykorzystywane do znajdowania defektów i luk w opracowywanym kodzie. Kluczem do zabezpieczenia

działań związanych z rozwojem oprogramowania37 jest ustanowienie standardowej kultury korporacyjnej i odpowiednich zasad, które:

* Postaw programistów zajmujących się bezpieczeństwem oprogramowania przy stole, gdy zostaną ustalone wymagania projektu oprogramowania,

* Uwzględnij zabezpieczenia w oprogramowaniu już na etapie projektowania,

* Zawierać wyłącznie przeskanowane pod kątem luk komponenty oprogramowania innych firm38 i korzystać z dynamicznie dołączanych bibliotek, tak aby najnowsze, mniej podatne na ataki i zaktualizowane komponenty oprogramowania automatycznie zastępowały starsze, przestarzałe i bardziej podatne na ataki oprogramowanie,

* Wspieranie współpracy i wzajemnego sprawdzania rozwoju oprogramowania,

* Włączyć lepsze testowanie na wczesnym etapie i przez cały cykl życia oprogramowania, aby zarządzać błędami w zakresie bezpieczeństwa i jakości podczas pisania kodu, oraz

* Ustanawiaj formalne procesy przekazywania informacji zwrotnych, których celem jest wyeliminowanie pierwotnych przyczyn luk w zabezpieczeniach, defektów i wad oprogramowania.

Takie działania podnoszą jakość kodu przed wydaniem kodu do produkcji. Kod o wyższej jakości ma zwykle mniej luk w zabezpieczeniach, mniejsze powierzchnie ataku i mniej dziur, które należy załatać, gdy oprogramowanie osiągnie stan produkcyjny. Jeśli zasoby do testowania wewnętrznego są ograniczone, usługi testowania bezpiecznego oprogramowania można zlecić zewnętrznym firmom, takim jak Coverity, która zapewnia platformę do testowania programistycznego lub NCC Group, która świadczy usługi testowania bezpośredniego. Idąc nawet dalej niż tylko skupiając się na nauce o tworzeniu oprogramowania, wielu szuka bardziej formalnych standardów rozwoju produktu, które zapewniają powtarzalne, proaktywne procesy rozwoju i testowania produktu. Niektórzy dostawcy, tacy jak Microsoft (w 2002 r.), za pośrednictwem inicjatywy Trustworthy Computing Initiative i Adobe (w 2009 r.), zainicjowali najnowocześniejsze, standardowe, wewnętrzne inicjatywy mające na celu włączenie zabezpieczeń do projektów ich oprogramowania przed masową produkcją i sprzedażą ich oprogramowania. Cykl życia oprogramowania Security Development Lifecycle39 (SDL) firmy Microsoft określa procesy tworzenia bezpiecznego oprogramowania. Niedawno, międzynarodowa norma ISO/IEC 27034-1 z 2011 r. określa wymagania i opisuje procesy i praktyki dotyczące bezpiecznego tworzenia oprogramowania. Kilka dużych firm produkujących oprogramowanie zaczyna używać tego standardu do uruchamiania kompleksowych programów mających na celu włączenie bezpieczeństwa do swoich produktów od samego początku etapu projektowania oprogramowania. Norma ta jest cenna zarówno dla nabywców, jak i konstruktorów produktów związanych z bezpieczeństwem. Twórcy oprogramowania wykazują należytą staranność w stosowaniu standardu do tworzenia wysokiej jakości, bezpiecznego kodu. Kupujący rozumieją, że twórcy oprogramowania zgodnego z przepisami są zobowiązani do zabezpieczania procesów programistycznych. Materiały szkoleniowe konsorcjum Software Assurance Forum for Excellence in Code (SAFECode) pozwalają twórcom produktów być na bieżąco z najlepszymi praktykami, zasadami i metodami inżynierii i rozwoju bezpiecznego oprogramowania. Inne organizacje, takie jak Association for Software Testing, również próbują zbudować społeczność programistów znających się na nauce o tworzeniu oprogramowania i testowaniu. Program Building Security in Maturity Model (BSIMM) umożliwia przedsiębiorstwom — jako połączonej społeczności — przeprowadzanie ankiet wśród swoich członków w celu rozpoznania wspólnego rdzenia najlepszych praktyk w zakresie bezpiecznego tworzenia oprogramowania. BSIMM stworzył de facto bezpieczny standard tworzenia oprogramowania, porównując rzeczywiste

bezpieczne środowiska kodowania i praktyki swoich członków, aby zidentyfikować najlepsze praktyki bezpiecznego tworzenia oprogramowania. Model jest darmowy na licencji Creative Commons.

Problemy w praktykach rozwojowych

Rozczarowującą obserwacją związaną z bezpiecznymi praktykami programistycznymi jest to, że badanie przeprowadzone w 2013 r.40 wykazało, że tylko około jedna trzecia twórców produktów skupia się na wbudowaniu bezpieczeństwa w swoje oprogramowanie; prawie dwie trzecie z nich niekoniecznie koncentruje się na bezpieczeństwie i nie rozważa korzystania ze standardowych technologii ograniczających ataki na aplikacje, takich jak zapobieganie wykonywaniu danych (DEP) i losowanie układu przestrzeni adresowej (ASLR). Sytuacja może się pogorszyć, jak np.

* Pojawiają się nowe tak zwane zwinne metodologie tworzenia i testowania oprogramowania,

* Zapotrzebowanie na bardziej złożone, oparte na chmurze lub mobilne oprogramowanie rośnie - często z większą gęstością podatności na ataki i

* Oprogramowanie Fielded jest aktualizowane - często poprzez mozaikę kodu stworzoną przez różnych programistów o różnych umiejętnościach, z różną wiedzą na temat aktualizowanego oprogramowania iw różnych momentach.

Wydaje się, że konsumenci chcą produktów o większej liczbie funkcji; a sprzedawcy wydają się mieć niewielką motywację lub narażenie na odpowiedzialność, aby inwestować dużo czasu lub zasobów w tworzenie solidnych produktów.

Nieformalne podejścia do oceny produktów

Różnorodne podejścia do oceny produktów nie są zależne od formalnych, standardowych, uznanych na całym świecie podejść do testowania i oceny bezpieczeństwa. Rzeczywiście, większość z nich nie osiągnęła statusu nawet de facto standardu, niemniej jednak są one uważane za kompletność. Takie podejścia obejmują:

* Deklaracje własne dostawcy (sekcja 51.4.4.1)

* Oceny konsumenckie (sekcja 51.4.4.2)

* Oceny oparte na konsorcjach (sekcja 51.4.4.3)

* Niejawne oceny poprzez tworzenie kodu open source (sekcja 51.4.4.4)

* Niejawne oceny poprzez hakowanie (sekcja 51.4.4.5)

* Oceny czasopism i publikacji w prasie branżowej (sekcja 51.4.4.6)

* Oceny handlowe stron trzecich przy użyciu metod de iure (sekcja 51.4.4.7)

Większość z tych podejść ma wady. Uważa się, że niektóre nie oferują dużej wartości. Jednym z podstawowych mankamentów jest to, że brak oparcia się na formalnych normach utrudnia porównywanie wyników oceny produktów:

* Różnych produktów,

* W przypadku produktów testowanych i ocenianych różnymi metodami oraz

* W przypadku produktów testowanych i ocenianych przez różne ośrodki badawcze, z których wszystkie rzekomo stosują to samo podejście do oceny produktów.

Deklaracje własne dostawcy

Podejście do budowania zaufania opiera się na pojęciu deklaracji własnych dostawców. Sprzedawca może jednostronnie twierdzić, że określony produkt spełnia potrzeby w zakresie bezpieczeństwa określonej klasy klientów i że zaimplementowane funkcje bezpieczeństwa produktu mogą wzbudzić odpowiednią dozę zaufania pożądanego przez klienta. Po części zaufanie związane z tym podejściem jest pośrednio związane z reputacją sprzedawcy w przeszłości lub z przeszłymi doświadczeniami klienta w kontaktach ze sprzedawcą. Jeśli reputacja dostawcy lub doświadczenia klientów są dobre, istnieje pewne poczucie, że sprzedawca ponownie wykonał odpowiednią pracę, wdrażając zabezpieczenia. W podejściu tym brakuje jednak wymiernych sposobów ilościowego określenia stopnia zaufania, jakie można powiązać z produktem. Brakuje również wymiernych sposobów porównywania względnych stopni zaufania, które można powiązać z różnymi produktami. Przykład takiego oświadczenia własnego został niedawno stworzony przez dział konsultingowy dużej firmy komputerowej41. W tym przykładzie sprzedawca określił najważniejsze kryteria wyboru dostawcy zarządzanych usług bezpieczeństwa (MSSP) i ujawnił, dlaczego usługi sprzedawcy są najlepsze na rynku. Takie podejście do samodeklaracji może mieć pewną zaletę w budowaniu poczucia ciągłego zaufania do produktów, które zostały zaktualizowane od czasu wcześniejszej wersji produktu, która przeszła rygorystyczne, oparte na standardach testy i oceny bezpieczeństwa. Jeśli wiadomo, że dostawca ma dobre możliwości w zakresie inżynierii bezpieczeństwa — takie, które można częściowo ocenić za pomocą standardowych metod podejścia do modelu dojrzałości zdolności (patrz sekcja 51.4.2.1) — i jeśli dostawca może przedstawić rozsądne dowody co do charakteru aktualizacji lub nowelizacja od wersji produktu, która została poddana rygorystycznej ocenie, może istnieć pewien jakościowy (aczkolwiek ilościowo nieznany) stopień pewności co do zaktualizowanego lub zmienionego produktu. W tych warunkach klienci, którzy mają wrodzone zaufanie do sprzedawcy, mogą sądzić, że jakość zmienionego produktu jest zbliżona do jakości wersji produktu, która została formalnie oceniona.

Oceny konsumenckie

Zgłoszono, że mniej niż 20 procent konsumentów oprogramowania ocenia asystenta bezpieczeństwa za pomocą aplikacji oprogramowania, które kupują. Konsumenci produktów mogą jednak samodzielnie wypracować niezbędną specjalistyczną wiedzę techniczną, aby bezpośrednio testować i oceniać określone produkty o zwiększonym poziomie bezpieczeństwa. Dostępne są standardowe narzędzia dostawców, które pomagają konsumentom w określonych obszarach technologii bezpieczeństwa. Na przykład dział GFI Software opracował Podręcznik oceny oprogramowania antywirusowego, który określa powtarzalne, łatwe do wdrożenia kryteria testowania dla klientów w celu oceny produktów antywirusowych dostawcy.42 Innym przykładem jest Ixia, która opracowała symulator ataku, który może uruchomić użytkownik produktów zabezpieczających w bezpiecznym środowisku, aby emulować szereg scenariuszy ataków lub konfiguracji, aby ocenić, jak dobrze dane produkty zabezpieczające wykrywają i blokują określone ataki43. Na przykład ataki botnetów zombie, a także scenariusze pełnego cyklu życia ataków DDoS mogą być symulowane. Alternatywnie, ze względu na wewnętrzną wiedzę fachową lub dostępny personel, konsumenci mogą zatrudnić konsultanta do przeprowadzenia ograniczonej oceny bezpieczeństwa za pomocą technik, takich jak testy penetracyjne lub analiza kodu źródłowego lub analiza binarna, gdy kod źródłowy nie jest dostępny. Konsumenci dysponujący większymi zasobami mogą zlecić niezależnemu podmiotowi oceniającemu, takiemu jak komercyjny dostawca testów bezpieczeństwa (np. testowanie i ocena. Wiele podejść stron trzecich ma charakter prywatny i wydaje się być unikalny. Niektóre instytucje finansowe zastosowały metodę oceny wewnętrznej. Instytucje finansowe jako całość bardzo dbają o to, aby produkty, z których korzystają, były godne zaufania. Bezpieczeństwo, integralność i solidność wszystkich produktów i systemów wspierających instytucje finansowe muszą być spójne i

weryfikowalne. Instytucje te obawiają się, że każde naruszenie bezpieczeństwa IT w dowolnym miejscu w ich systemach spowoduje utratę zaufania do całej instytucji, a nie tylko do konkretnego, podważonego produktu informatycznego. Wiele instytucji finansowych opracowało własne wewnętrzne standardowe specyfikacje bezpieczeństwa i procesy oceny, a także metodologię oceny w celu ilościowego określenia, porównania, zatwierdzenia i certyfikacji ogólnych aspektów bezpieczeństwa konkurencyjnych produktów. Jedną z konsekwencji tego podejścia dla całej społeczności klientów jest to, że wymaga ono znacznego, kosztownego powielania infrastruktury testowej w całej branży finansowej, a także kosztownego powielania wysiłków w zakresie wsparcia testowania przez dostawców produktów, które są kandydatami do zakupu przez wielu klienci. Gdy każdy podmiot finansowy finansuje ustanowienie własnego programu testowania, łączne wydatki na testowanie rosną we wszystkich podmiotach w branży finansowej. Ponadto, ponieważ liczba urządzeń finansowych, takich jak platformy kart kredytowych, systemy operacyjne i tysiące aplikacji, stale rośnie dramatycznie, wewnętrzne zasoby mają trudności z nadążaniem. Klienci produktów uważają, że tego rodzaju samodzielne, wewnętrzne podejście do testowania jest ogromnym przedsięwzięciem pod względem rozwoju, wdrożenia, demonstracji zasadności, konserwacji i ponownego uzasadnienia. Stwierdzili, że jest to kosztowne, czasochłonne, wymagające dużych zasobów, trudne w utrzymaniu, zawsze otwarte na interpretację i debatę oraz zawsze wymagające uzasadnienia dla organów regulacyjnych i zleceniodawców na nowych rynkach.

Podejścia do oceny oparte na konsorcjach

Istnieje lub istniało wiele podejść kierowanych przez konsorcja w celu wykazania interoperacyjności produktu lub zgodności produktu z określonymi funkcjami bezpieczeństwa lub określonymi standardami technologii bezpieczeństwa. W świecie Internetu pojęcie przestojów wdrożeniowych wśród próbnych (przedproduktowych) wdrożeń powstających standardów IETF jest ostoją społeczności od dłuższego czasu. Na przykład IETF zainicjował serię warsztatów dotyczących interoperacyjności IPSec VPN po ukoronowaniu standardu Internet Key Exchange Version 2 (IKEv2). Dostawcy preproduktów opartych na IKEv2 zebrali się we wspólnym ośrodku testowym, aby przetestować funkcjonalność i interoperacyjność swoich preproduktów w tym swoich konkurentów. Początkowe scenariusze testowe koncentrowały się na podstawowej funkcjonalności i bezpiecznej konserwacji tunelu. Inne konsorcja stosują własne lub standardowe metody testowania.

Konsorcjum wirtualnej sieci prywatnej

Konsorcjum Virtual Private Network (VPN) opracowało podejście do wykazywania zgodności produktu z określonym standardem bezpieczeństwa. Konsorcjum VPN przeprowadza testy implementacji IPSec i Secure Sockets Layer (SSL) zbudowanych przez członków konsorcjum. Na początku XXI wieku konsorcjum dostarczyło trzy konkretne profile testów zgodności produktów VPN wdrażających standard IPSec IETF. Dla każdego typu profilu testowego wstępnie zdefiniowane zadania musiały zostać pomyślnie wykonane na dwóch różnych referencyjnych bramkach testowych. Ze względu na niewyczerpujący zestaw testów, pomyślny wynik testu zgodności konsorcjum VPN dostarczył jedynie wskazówek, że testowane produkty są zgodne, w ograniczonej części, z różnymi standardowymi częściami standardu IPSec. Testy te dostarczyły również wskazówek, że interoperacyjność może być możliwa z innymi produktami, które pomyślnie przejdą te same testy w tych samych warunkach środowiskowych. Od tego czasu konsorcjum skupiło się na testowaniu interoperacyjności. Przeprowadza kilka klas testów interoperacyjności IPSec: Basic Interoperability, AES Interoperability, IKEv2 Basic Interoperability, IPv6 Interoperability oraz Authentication with Certificates Interoperability. Określono typy testowanych możliwości oraz profile, według których testowane systemy są konfigurowane dla każdej klasy testów interoperacyjności. Testy pomagają zapewnić użytkownikom sieci VPN, że systemy IPSec skonfigurowane zgodnie z określonym profilem są ogólnie

kompatybilne z innymi systemami IPSec również skonfigurowanymi zgodnie z tym samym profilem. Konsorcjum zapewnia również testy interoperacyjności profili różnych funkcji SSL VPN w implementacjach SSL. Konsorcjum wystawia logo dla produktów firm członkowskich, które współpracują z co najmniej 75 procentami innych produktów w teście interoperacyjności. Utrzymywana jest lista firm członkowskich, które oferują produkty, które pomyślnie przejdą określone testy interoperacyjności.

Sojusz bezpieczeństwa w chmurze

CSA ustanowiła publicznie dostępny rejestr bezpieczeństwa, zaufania i pewności.46 Każdy dostawca usług w chmurze może publikować samooceny, które dokumentują praktyki bezpieczeństwa dostawcy usług w chmurze i ich zgodność z najlepszymi praktykami CSA. Samooceny dostawców usług w chmurze są dokumentowane (a) zgodnie ze standardowym kwestionariuszem CSA Cloud Assessment Initiative Questionnaire lub (c) za pośrednictwem macierzy CSA Cloud Controls Matrix, która szczegółowo opisuje koncepcje i zasady bezpieczeństwa dostawcy usług w chmurze zgodnie z wytycznymi bezpieczeństwa CSA.

Grupa użytkowników zabezpieczeń kart inteligentnych

Chociaż indywidualne, wewnętrzne metody były pierwotnie stosowane przez poszczególne instytucje finansowe do oceny tysięcy finansowych produktów, komponentów i systemów IT, społeczność finansowa połączyła się jako całość w grupie Smart Card Security Users Group. Dzięki tej grupie instytucje finansowe mogą stosować jeden standard - CC - do oceny produktów i unikać powielania swoich indywidualnych wysiłków związanych z oceną produktów. Korzyści z takiego sojuszu obejmowały:

* Instytucje finansowe mogą zastąpić swoje wewnętrzne, niestandardowe podejście do oceny produktów wspólną, powszechnie akceptowaną metodą.

* Mogą połączyć swoje zasoby, aby sprostać powszechnym potrzebom w zakresie testowania i oceny bezpieczeństwa, stosując oparte na standardach specyfikacje bezpieczeństwa CC i schematy testowania uznawane przez wszystkich głównych graczy finansowych.

* Potrafi opracować profile wymagań bezpieczeństwa dla różnych wspólnych elementów kart inteligentnych (np. chipów, systemów operacyjnych, aplikacji, silników kryptograficznych).

* Mogą opracowywać wspólne zestawy testów w celu ujednolicenia obecnej mieszanki fragmentarycznych testów kart inteligentnych dostosowanych do potrzeb klientów i dostawców.

* Mogą zlecić testowanie i ocenę bezpieczeństwa kompetentnym, akredytowanym laboratoriom badawczym, z których wiedzy mogą korzystać wszystkie instytucje finansowe.

Sojusz stworzył profil CC — tak zwany profil ochrony kart inteligentnych - obejmujący standardowe wymagania funkcjonalne dotyczące bezpieczeństwa i wymagania dotyczące gwarancji, które mają być spełnione przez karty inteligentne używane w połączeniu z wrażliwymi aplikacjami, takimi jak te spotykane w systemach płatności w branży bankowej. Ten standardowy profil wymagań został zatwierdzony i certyfikowany przez Canadian CC Scheme i może być używany w całej społeczności finansowej. Od tego czasu opracowano brytyjski profil ochrony kart inteligentnych dla kart uwierzytelniających z dwoma interfejsami do zastosowań takich jak paszporty. Konsumenci mogą odwoływać się do takich profili, aby określić swoje wymagania. Dostawcy mogą odwoływać się do takich profili, aby wskazać, co zbudowali. Akredytowane laboratoria badawcze stosują standardowe metody, aby przetestować poszczególne produkty raz dla całej społeczności konsumenckiej (nie raz na

instytucję konsumencką). Standardowe testy oceniają twierdzenie dostawcy, że jego produkt spełnia standardowy profil wymagań. Konsument ze znaną pewnością może następnie kupić dowolny oceniany produkt, który został niezależnie certyfikowany pod kątem zgodności z określonym profilem ochrony.

Podejście open source

Jednym z podejść do tworzenia oprogramowania jest wykorzystanie modelu Open Source. Zgodnie z tym podejściem oprogramowanie jest udostępniane publicznie do wglądu, modyfikacji wad i nieefektywności oraz ewentualnej aktualizacji możliwości i funkcji. Teoretycznie dzięki ciągłym i kolektywnym – ale nieskoordynowanym i pozornie przypadkowym – wysiłkom potencjalnie tysięcy niezależnych programistów i testerów, publiczna ocena poprawi z czasem jakość oprogramowania. Wadą podejścia open source jest to, że stopień wiarygodności osiągnięty przez ten proces jest niemierzalny. W niektórych przypadkach zaobserwowano, że główni dostawcy oprogramowania (zwłaszcza ci, którzy mają produkty zależne od korygowanego oprogramowania open source) agresywnie dążą do usunięcia luk w zabezpieczeniach; podczas gdy inni twórcy oprogramowania są bardziej skłonni do rozszerzania funkcjonalności oprogramowania open source niż do naprawiania wykrytych luk w zabezpieczeniach. Aby pomóc zidentyfikować problemy z bezpieczeństwem w otwartym kodzie źródłowym, Departament Bezpieczeństwa Wewnętrznego Stanów Zjednoczonych zainicjował projekt Open Source Hardening dotyczący wykrywania i naprawiania luk w zabezpieczeniach. W ramach tego projektu opracowano nowe podejścia do znajdowania krytycznych defektów w złożonych zestawach kodu oprogramowania i zastosowano je do testowania otwartego kodu źródłowego w celu wyizolowania defektów i pierwotnych przyczyn. W nowszym podobnym przedsięwzięciu50 projekt Eliminate Vulnerable Code (eVc) wykorzystuje narzędzia do przeszukiwania Internetu, a także identyfikację ochotników i/lub przesyłanie złego kodu w celu odkrycia przykładów lub cytatów z podatnego na ataki otwartego kodu źródłowego. Takie odkrycia są dodawane do listy udostępnianej członkom eVc oraz twórcom wykrytego wadliwego oprogramowania. Projekt eVc ma nadzieję, że członkowie eVc, sponsorzy, środowisko akademickie i inne osoby mogą współpracować z twórcami wykrytego wadliwego oprogramowania w celu naprawy lub usunięcia wadliwego, podatnego na ataki oprogramowania. Eliminując wadliwy kod open source, innym projektom open source łatwiej będzie ponownie wykorzystać kod wyższej jakości, który nie zawiera luk w zabezpieczeniach, takich jak te zidentyfikowane na liście 10 największych wad Open Web Application Security Project (OWASP) Top 10 w zabezpieczeniach aplikacji internetowych skaz52 lub na liście SANS Top 25 wad.

Jednak wiarygodność produktu to coś więcej niż tylko ulepszony kod. Chociaż kod open source będzie miał pewien stopień wiarygodności opracowany w procesie open source, włączenie takiego kodu do produktu nadal prowadzi do innych czynników, które wpływają na wiarygodność produktu. Wiarygodność produktu zależy również od procesów dostawcy, takich jak jakość projektu, ochrona zapewniona funkcjom bezpieczeństwa podczas dostawy produktu od sprzedawcy do konsumenta, strategie dostawcy dotyczące utrzymania lub aktualizacji zabezpieczeń w obliczu nowych zagrożeń itp. NA. Kilku dostawców polegało na standardowym podejściu do testowania i oceny CC, aby ocenić funkcje bezpieczeństwa i zapewnienia bezpieczeństwa swoich produktów oprogramowania dla systemu Linux. Listę ocenianych produktów Linux, które są certyfikowane zgodnie z podejściem CC, można znaleźć w Internecie.

Hakowanie

De facto zapewnienie podstawowego bezpieczeństwa produktu może wynikać z tych, którzy aktywnie badają nowe produkty pod kątem luk w zabezpieczeniach. Takie sondowanie może wynikać z

usankcjonowanych wewnętrznie sondowań bezpieczeństwa lub z nieusankcjonowanych, nieoczekiwanych sondowań przeprowadzanych przez osoby o złej woli. Podejścia hakerskie (etyczne lub inne) niekoniecznie są zgodne ze spójnym lub kompleksowym podejściem do oceny jakości wdrożonych funkcji i usług bezpieczeństwa. W związku z tym osiągnięty poziom pewności jest nieznany i zazwyczaj bardzo niski.

Prasa branżowa

W wielu branżowych publikacjach prasowych i magazynach zamieszczane są recenzje produktów związanych z bezpieczeństwem. Produkty są testowane w środowiskach ad hoc i według prywatnych, ad hoc, kryteriów de iure, które różnią się w zależności od produktu i czasopisma. Takie magazyny mogą polegać na nieakredytowanych konsultantach, pracownikach lub prywatnych laboratoriach w celu przeglądu produktów. Niektóre recenzje mogą skupiać się na badaniu ilościowych szczegółów produktu innych niż bezpieczeństwo, takich jak wydajność lub przepustowość produktu. Przeprowadzane testy często nie wystarczają do oceny rzeczywistych aspektów bezpieczeństwa produktu. Niektóre recenzje oceniają parametry jakościowe, takie jak innowacyjność produktu. Ze względu na potencjalny brak skwantyfikowanego rygoru testowania i potencjalną odmienność wskaźników oceny, porównania recenzji prasy branżowej z różnych źródeł są trudne. Być może najważniejsze jest to, że nie dokonuje się oceny zaufania (zapewnienia), które można powiązać z solidnością wdrożenia zabezpieczeń. Przykłady publikacji zawierających recenzje produktów zabezpieczających to magazyn SC (dawniej Secure Computing),55 Network Computing,56 magazyn Security Management,57 InfoWorld58 i wiele innych. Niektóre z tych branżowych inicjatyw prasowych podsumowano poniżej.

Magazyn SC

W swoim ogólnym procesie testowania poszczególnych produktów związanych z bezpieczeństwem SC Magazine wykorzystuje około 50 prywatnych kryteriów opracowanych wspólnie przez SC Lab i Centrum Bezpieczeństwa Regionalnego i Narodowego na Eastern Michigan University. Testy grup produktów skupiają się na cechach użytkowych. Metody testowania i oceny są podobne do tych stosowanych dla najniższych poziomów pewności CC. Magazyn SC ustalił również ogólne wartości ocen, aby wskazać, jak dobrze produkt spisał się w odniesieniu do kryteriów testu i czy produkt powinien być rozważany przy zakupie. Przykłady typów produktów lub grup produktów, które zostały sprawdzone przez SC Magazine, obejmują: SIEM, sieciowe urządzenia kryminalistyczne, uwierzytelnianie wieloskładnikowe, ujednolicone menedżery zagrożeń, menedżer ryzyka, strażnik sieci, platforma egzekwowania tożsamości, menedżer bezpieczeństwa aplikacji, menedżer haseł, Zapora sieciowa aplikacji, monitory aktywności baz danych, bezpieczna brama poczty e-mail i nie tylko. Pełniejsze listy przetestowanych pozycji znajdują się na stronie internetowej magazynu. Firma SC opracowała również przewodniki dla kupujących dotyczące grup produktów, takich jak rozwiązania Universal Single Sign-On. Magazyn SC publikuje również prywatne oceny produktów w określonych klasach, takich jak produkty do kontroli tożsamości w chmurze i kontroli dostępu, ujednolicone rozwiązania do zarządzania zagrożeniami, zapory ogniowe nowej generacji i nie tylko. Inne publikacje. ComputerWorld i IT Business Edge uzyskują prywatne oceny (często z tego samego biura oceny) produktów z różnych klas produktów związanych z bezpieczeństwem, takich jak produkty zabezpieczające punkty końcowe. Indywidualne oceny produktów są porównywane z innymi produktami w tej samej klasie produktów. W przypadku produktów z zabezpieczeniami kryteria testowe obejmują metryki wydajności wskazujące, w jaki sposób procesy związane z bezpieczeństwem mogą wpływać na ogólną wydajność systemu z włączonymi zabezpieczeniami. NetworkWorld uzyskuje prywatne przewodniki dla kupujących dotyczące technologii związanych z bezpieczeństwem, takich jak zarządzanie tożsamością w chmurach, narzędzia SSL/VPN i inne. Ocena opiera się na (a) deklaracjach

własnych dostawcy udzielonych prywatnie, pytaniach ankiety ewaluacyjnej częściowo ukierunkowanej na funkcje bezpieczeństwa oraz (b) praktycznej konfiguracji produktów przez osobę oceniającą. InformationWeek tworzy przewodniki dla kupujących dotyczące technologii, takich jak produkty chroniące przed złośliwym oprogramowaniem typu gateway. Ocena opiera się na deklaracjach własnych dostawcy w odpowiedzi na prywatne pytania w ankiecie ewaluacyjnej, częściowo zorientowanej na funkcjonalność zabezpieczeń. IT Whitepapers uzyskuje prywatne porównania produktów lub usług związanych z bezpieczeństwem. Niedawne porównania ocen obejmowały na przykład (a) przepisy bezpieczeństwa na głównych platformach mobilnych oraz (b) dostawców zarządzanych usług bezpieczeństwa.

Podejścia do komercyjnej oceny de jure stron trzecich

Na początku na arenie oceny bezpieczeństwa zewnętrzne, komercyjne podejścia do oceny bezpieczeństwa były czasami przeprowadzane przez nieakredytowane domy testowe lub firmy konsultingowe. Te strony trzecie zapewniły stosunkowo niskie zaufanie, tak zwane testy na poziomie powierzchni. Dzięki takim testom dostawcy produktów związanych z bezpieczeństwem otrzymywali albo znak firmowy, albo niezależny raport oceniający sporządzony przez stronę trzecią, do którego można się odwoływać w broszurach i reklamach produktów dostawców. Taka działalność komercyjna rozpoczęła się w czasie, gdy potrzebna była tańsza – choć mniej wiarygodna – alternatywa dla kosztownych, długotrwałych, ekonomicznie nieodpowiednich ewaluacji rządowych, takich jak tak zwane ewaluacje pomarańczowej księgi . Te działania związane z oceną handlową były również dostępne w celu wsparcia badań prasy branżowej i recenzji produktów w czasopismach. Takie niestandardowe, zewnętrzne podejścia są nadal powszechne. Opierając się na takich podejściach, można osiągnąć pewną jakościową redukcję ryzyka. Zazwyczaj opierają się one na prostych, uniwersalnych testach, które zwykle zapewniają minimalne, pobieżne sprawdzenie niektórych zaimplementowanych funkcji bezpieczeństwa. Niektóre z tych testów koncentrują się na szczegółach produktu innych niż bezpieczeństwo, takich jak wydajność lub przepustowość. Nie dokonuje się oceny zaufania (zapewnienia), które można powiązać z solidnością wdrożenia zabezpieczeń. W najlepszym przypadku są to podejścia typu „czarna skrzynka", w których produkty można badać wyłącznie na podstawie ich wyników w odniesieniu do bodźców. Podejścia te nie dają możliwości oceny w oparciu o podstawowy projekt produktu lub zasady inżynieryjne zastosowane przez dostawcę do zbudowania produktu. Niemniej jednak wielu dostawców poddaje się tego rodzaju testom komercyjnym z powodu presji ze strony produktów ich konkurentów, którzy są w ten sposób testowani. Koszty testów są rozsądne, ale takie testy nie dostarczają konsumentom danych wejściowych (np. raportów z oceny), które można by przeanalizować w celu zróżnicowania produktów. Bardziej wszechstronne produkty nie są badane pod kątem żadnej z ich różnicujących możliwości. Zamiast tego takie programy testowania ze znacznikami wyboru zapewniają jedynie wspólny mianownik oceny produktów. Typową reakcją dostawców na tego typu niestandardowe oceny stron trzecich i programy brandingowe jest to, że często nie są one zbyt dobre i często rozpraszają uwagę. Sprzedawcy wskazują również, że w przeciwieństwie do bardziej rygorystycznego, opartego na standardach paradygmatu testowania, takiego jak ten oparty na CC, te niestandardowe programy innych firm nie mają procesów pomagających poprawić jakość testowanego produktu. W przeciwieństwie do laboratoriów testujących CC wielu dostawców nie postrzega tych niestandardowych laboratoriów testowych jako partnerów strategicznych, którzy chcą ulepszyć testowany produkt. Przykłady tego typu podejść do oceny produktów obejmują program znaczników kontrolnych West Coast Labs , certyfikowany program ICSA Labs i kilka innych .

Program znaczników wyboru

Program Check Mark to prywatna usługa testowania świadczona przez West Coast Labs (www.westcoastlabs.org). Chociaż reklamuje się stosowanie standardowych kryteriów testowania w standardowym podejściu do testowania, program Check Mark ustanawia prywatne kryteria i prywatną metodologię testowania, które nie są uznawane przez legalne organy normalizacyjne, takie jak ISO. Prywatne kryteria i podejścia testowe West Coast mają zastosowanie do niektórych typów komputerów -produkty zabezpieczające, takie jak produkty antywirusowe, produkty firewall i produkty VPN. Kryteria mają na celu osiągnięcie podstawowego poziomu ochrony przed szeregiem powszechnych wrogich ataków. West Coast Labs testuje produkty pod kątem odpowiednich kryteriów Check Mark i, jeśli testy wypadną pomyślnie, wydaje certyfikat, który pokazuje, że określone wersje produktów spełniają określone Check Mark kryteria.

Certyfikat ICSA Labs

Inną dobrze znaną komercyjną usługą znakowania produktów związaną z bezpieczeństwem jest program certyfikacji produktów prowadzony przez ICSA Labs60. Podejście ICSA jest podobne do podejścia testowego West Coast Labs. Wydajność produktu jest testowana według określonych kryteriów, aby ocenić, czy produkt jest odporny na typowe rodzaje zagrożeń i ryzyka określone w kryteriach testowania. Testowanie produktów jest zazwyczaj podejściem zorientowanym na listę kontrolną, przeznaczonym dla testerów, którzy nie są ekspertami. Kryteria testowania są opracowywane dla wielu klas produktów, takich jak zapory ogniowe i oprogramowanie antywirusowe (AV). Podczas gdy Check Mark wykorzystuje prywatne kryteria testowania, ICSA stosuje tak zwane kryteria publiczne. Te kryteria publiczne są jednak niestandardowe, podobnie jak kryteria Check Mark, ponieważ są tworzone poza uznanymi krajowymi lub międzynarodowymi społecznościami zajmującymi się opracowywaniem standardów. Zamiast tego kryteria testowania ICSA są opracowywane przez zaproszonych członków. Produkty spełniające kryteria ICSA są uprawnione do umieszczania znaku marki ICSA. Produkty, które się nie powiodły, są zgłaszane ich dostawcom wraz ze szczegółową analizą kryteriów, których nie spełniły. W przeciwieństwie do certyfikatu Zachodniego Wybrzeża, po przyznaniu produktom certyfikatu ICSA dostawcy przyjmują na siebie obowiązek samokontroli i samodzielnego deklarowania ciągłej certyfikacji ewolucji określonej wersji produktu, która przeszła testy ICSA. Wyrywkowe kontrole przeprowadzane przez ICSA służą do sprawdzenia, czy obecnie wysyłane produkty nadal mogą przejść testy ICSA.

Inne oceny i rzeczoznawcy stron trzecich

Istnieje kilka innych organizacji, które wykorzystują prywatne, nieformalne metody do tworzenia zewnętrznych ocen niektórych rodzajów produktów lub usług bezpieczeństwa. Oto przykłady.

* Firma Gartner publikuje analizy Magic Quadrant, które oceniają, jak dobrze produkt wypada w porównaniu z innymi produktami z tej samej klasy produktów i gdzie znajduje się produkt w Magic Quadrant właściwości. Istnieją przykłady analiz Magic Quadrant dla klas produktów, takich jak Unified Threat Management.

* Forrester wystawia oceny produktów i usług w tej samej klasie usług. Na przykład 15-kryteriowa ocena 10 dostawców zarządzanych usług bezpieczeństwa została przeprowadzona przy użyciu prywatnych kryteriów oceny.

* Firma NSS Labs korzysta z własnego laboratorium badawczego zamiast ankiet i kwestionariuszy do tworzenia przewodników po najlepszych praktykach, recenzji produktów, raportów z testów porównawczych, przewodników dla kupujących i nie tylko. Takie materiały dotyczą zabezpieczeń lub urządzeń obsługujących zabezpieczenia, takich jak na przykład przeglądarki internetowe, zapory ogniowe aplikacji internetowych, zapory ogniowe nowej generacji, rozwiązania dla punktów

końcowych, systemy wykrywania naruszeń bezpieczeństwa, systemy zapobiegania włamaniom, produkty antywirusowe i inne. Kryteria testu są prywatne i dostosowane do oceny, która ma zostać przeprowadzona. Mogą one obejmować testy weryfikujące stabilność, wydajność i skuteczność bezpieczeństwa urządzenia (np. czy zapora sieciowa nie blokuje legalnego ruchu). Testy mogą określić dokładność zabezpieczenia urządzenia, a także użyteczność urządzenia. NSS Labs publikuje swoje metodologie testowe dla konkretnych urządzeń, a także własne badania dotyczące skuteczności zabezpieczeń. Publikuje również raporty o zagrożeniach związanych z lukami w zabezpieczeniach. Materiały badawcze NSS są dostępne przede wszystkim dla klientów abonamentowych.

* Veracode to kolejna zewnętrzna osoba oceniająca dostępna dla konsumentów, którzy nie są w stanie obsługiwać sensownego programu do testowania aspektów bezpieczeństwa produktów dostawcy. Aby zaspokoić potrzeby konsumentów w zakresie testowania bezpieczeństwa, firma Veracode ustanowiła program Veracode Vendor Application Security Testing (VAST). W połączeniu z opartą na chmurze platformą testową, Veracode zapewnia analizę wartości bezpieczeństwa oprogramowania aplikacji dostawcy i jego zgodności z politykami bezpieczeństwa klienta i wymaganiami dotyczącymi oprogramowania aplikacji, które kupują. Zapewnia również de iure, oparte na standardach wymagania punktowe na poziomie pewności, które określają minimalny zestaw testów, które należy wykonać. Podobnie jak paradygmat CC, Veracode stara się nawiązać partnerską relację z dostawcami. Ujawnia swoje wyniki testów dostawcom i przekazuje wskazówki dotyczące naprawy programistom. Dostępny jest doskonały opis procesów oceny bezpieczeństwa, które należy wykonać w połączeniu z programem VAST.

* AV-Test Institute przeprowadza analizy produktów zabezpieczających lub komponentów63. Wykonuje również testy porównawcze lub testy oprogramowania w wersji beta. Oceny wykorzystują codziennie powiększane złośliwe i bezpieczne próbki danych testowych AV-Test oraz własne narzędzia analityczne, a także prywatne kryteria testowe. Kryteria opierają się na ochronie (w tym np. ochronie przed atakami szkodliwego oprogramowania typu zero-day), naprawie (np. w zakresie wydajności w wykrywaniu i usuwaniu ukrytego szkodliwego oprogramowania) oraz użyteczności (w tym m.in. spowolnieniu wydajności komputerów korzystających z sprawdzone produkty). W oparciu o system punktacji zależny od wyników badań, Instytut przyznaje znaki certyfikacyjne. Recertyfikacja odbywa się okresowo. W prasie branżowej często pojawiają się wyniki testów porównawczych dla różnych klas produktów. Na przykład wyniki testów kilku skanerów antywirusowych dla systemu Windows 8 zostały niedawno podsumowane w prasie branżowej.

Standardy oceny bezpieczeństwa produktów

W przeciwieństwie do omówionych właśnie nieformalnych, niestandardowych podejść do oceny produktów, istnieją formalne standardy oceny różnych aspektów bezpieczeństwa związanych z produktami lub usługami. Jak wyszczególniono wcześniej, istnieją normy oceniające ogólną jakość i solidność konstruktorów produktów i ich organizację oraz określające solidne metody rozwoju dla konstruktorów produktów. Określenie solidności zabezpieczeń w oparciu o te standardy zazwyczaj prowadzi do uogólnionych wniosków, takich jak „dobrzy" dostawcy budują „dobre" produkty. Jak wyszczególniono w poniższych sekcjach, można zastosować inne standardy w celu oceny jakości produktu, jakości usług lub kombinacji zarówno jakości konstruktorów produktów, jak i jakości ich produktów. Te ostatnie standardy można wykorzystać do ilościowego określenia, jak dobrze „dobrzy" dostawcy budują „dobre" produkty (z możliwymi do zidentyfikowania i udowodnienia poziomami pewności), o ile „lepsi" poszczególni dostawcy mogą zbudować jeszcze „lepsze" produkty (z możliwymi do zidentyfikowania i udowodnienia, generalnie wyższymi poziomy bezpieczeństwa) oraz jak wszechstronne są funkcje bezpieczeństwa w ramach określonych klas produktów tworzonych przez

tych dostawców. Podobnie istnieje co najmniej jeden standard sprawdzania, czy „dobrzy" usługodawcy oferują „dobre" usługi.

STANDARDOWE METODY OCENY PRODUKTÓW I USŁUG

Rządowe standardowe programy walidacji kryptograficznej

Ewoluująca seria standardów FIPS 14065 określa wymagania, jakie mają spełniać moduły kryptograficzne. W systemach komputerowych i telekomunikacyjnych używanych lub zlecanych przez rząd federalny, rząd USA nakazuje stosowanie zatwierdzonych modułów kryptograficznych do wszystkich zastosowań kryptograficznych, które chronią „wrażliwe, ale jawne" informacje. FISMA eliminuje jakąkolwiek możliwość otrzymania zwolnienia z rządowego mandatu FIPS 140. Rząd kanadyjski wymaga stosowania takich modułów do ochrony „wskazanych informacji". Inne organizacje pozarządowe również chcą korzystać ze sprawdzonych, dostępnych na rynku modułów kryptograficznych. Standardy FIPS 140 stanowią podstawę długoletniego, popularnego Cryptographic Module Validation Program (CMVP).Program ten koncentruje się na testowaniu, ocenie, walidacji i certyfikacji sprzętowych i programowych modułów kryptograficznych. Moduł kryptograficzny może być elementem wbudowanym w produkt lub aplikację; lub może to być samodzielny produkt sam w sobie. Warunkiem wstępnym walidacji modułu kryptograficznego jest walidacja poprawnej i kompletnej implementacji standardowych algorytmów kryptograficznych stosowanych w modułach kryptograficznych. Zatwierdzone przez FIPS standardowe algorytmy klucza symetrycznego do szyfrowania obejmują Advanced Encryption Standard, który jest obecnie wybieranym algorytmem, Triple-DES i Skipjack. Cryptographic Algorithm Validation Program (CAVP) wykorzystuje zaprojektowane przez CAVP zestawy testów walidacyjnych do testowania, oceny i weryfikowania standardowych algorytmów kryptograficznych przy użyciu procesów i metodologii podobnych do opisanych poniżej dla CMVP. (Szczegółowe testy są opisane w towarzyszących standardach NIST.) Szczegóły dotyczące CAVP nie są tu podane. Wystarczy wskazać, że tysiące implementacji algorytmów kryptograficznych otrzymało dotychczas walidację algorytmów. FIPS 140-1 definiuje cztery rosnące, jakościowe poziomy zapewniania bezpieczeństwa, począwszy od najniższych wymagań określonych na poziomie 1 do bardziej sekwencyjnie addytywnych wymagań bezpieczeństwa na każdym z kolejnych wyższych poziomów. Wymagania bezpieczeństwa dotyczą 11 różnych obszarów związanych z projektowaniem i wdrażaniem modułu kryptograficznego. FIPS 140-2 i powstający FIPS 140-3 mają zastosowanie do bardziej współczesnych implementacji modułów kryptograficznych. Zawierają one zmiany w technologii modułów kryptograficznych, a w przypadku FIPS 140-3 dodają nowe wymagania i dodatkową gwarancję Poziom 5. Specjalne laboratoria testujące bezpieczeństwo przeprowadzają standardowe testy zgodności modułów kryptograficznych z wymaganiami określonymi w FIPS 140-2 lub FIPS 140-1 . Istnieje wiele takich niezależnych, komercyjnych, zewnętrznych, tak zwanych laboratoriów kryptograficznych i testujących zabezpieczenia - każde indywidualnie akredytowane przez Narodowy Dobrowolny Program Akredytacji Laboratoriów NIST (NVLAP). Podmioty, które chcą przeprowadzić walidację modułów kryptograficznych, muszą zawrzeć umowę z którymkolwiek z tych laboratoriów na usługę testowania modułów kryptograficznych i zweryfikować takie oceny. W odniesieniu do konkretnego testowanego modułu kryptograficznego laboratoria te mogą przeprowadzić odpowiednie, znormalizowane testy zgodności z zestawu standardowych testów zgodności68 dostosowanych do czterech poziomów bezpieczeństwa FIPS 140. Po potwierdzeniu, że wyniki testu przeprowadzonego przez akredytowane laboratorium testowe prawidłowo i całkowicie wykazują, że testowany moduł kryptograficzny jest zgodny z jednym ze standardów FIPS 140, certyfikat CMVP może zostać wydany przez NIST lub Communications Security Establishment Canada (CSEC). Certyfikat zawiera punktację oceny ustaloną na podstawie powyższych testów. NIST prowadzi listę repozytoriów modułów kryptograficznych – przeszłych i obecnych – które zostały przetestowane i

zweryfikowane. Należy zauważyć, że więcej produktów niż pojawia się w repozytorium zatwierdzonych modułów kryptograficznych może zawierać zatwierdzony moduł, który jest wymieniony w repozytorium. NIST prowadzi również listę modułów kryptograficznych, które są w trakcie oceny. Schemat testowania i walidacji FIPS 140 nie jest tak szeroki, elastyczny i dalekosiężny jak schemat CC , który jest również używany do ocena i certyfikacja produktów. Dlaczego? Ponieważ schemat FIPS 140 koncentruje się tylko na jednej klasie jednostek - modułach kryptograficznych - podczas gdy schemat CC ma zastosowanie do dowolnej klasy produktów, a także do szerszego zestawu możliwych wymogów dotyczących zapewnienia bezpieczeństwa w zakresie projektowania, wdrażania, wdrażania i konserwacja produktów. Ponadto wymagania bezpieczeństwa FIPS 140 nie są bezpośrednio odwzorowywane na żadne konkretne wymagania bezpieczeństwa CC. W związku z tym, gdy wymagany jest certyfikat FIPS 140, nie można zastąpić certyfikatu CC.

FedRAMP. Program FedRAMP to program rządu Stanów Zjednoczonych, który wspiera federalne agencje rządowe w przyjmowaniu komercyjnych lub rządowych usług w chmurze71. Takie usługi w chmurze mogą być świadczone zgodnie z jednym z kilku różnych modeli świadczenia usług, takich jak infrastruktura jako usługa (IaaS) lub Platforma jako usługa (PaaS). FedRAMP to inny rodzaj programu oceny i certyfikacji bezpieczeństwa rządu USA. Nie jest ukierunkowany konkretnie na produkty związane z bezpieczeństwem. Zamiast tego jest zorientowany na ocenę dostawców usług i stosowanych przez nich systemów w szczególności dostawcy usług w chmurze. Standardowe procesy FedRAMP przynoszą korzyści zarówno dostawcom usług w chmurze, jak i klientom usług w chmurze. Pojedyncza, zewnętrzna ocena roszczeń dostawcy usług w chmurze w zakresie bezpieczeństwa zmniejsza koszty oceny bezpieczeństwa dostawcy usług w chmurze, eliminując ponowną ocenę dla różnych klientów w chmurze. Pomyślne oceny otrzymują autoryzację rządową, która umożliwia dowolnej lub wszystkim agencjom rządowym korzystanie z oferty autoryzowanego dostawcy usług w chmurze. FedRAMP stosuje podejście oparte na standardach i ryzyku, które opiera się na:

1. Wymagania bezpieczeństwa Standardy, które wymagają od dostawców chmury wdrożenia funkcji bezpieczeństwa, które spełniają standardowe wymagania bezpieczeństwa FedRAMP.

2. Standardy oceny bezpieczeństwa, które wymagają od zatwierdzonych, niezależnych stron trzecich audytu i oceny ofert dostawcy usług w chmurze oraz opracowania raportu z oceny bezpieczeństwa.

3. Rządowe standardy autoryzacji, które są wykorzystywane przez Wspólną Radę Autoryzacyjną FedRAMP do przeglądania raportów z oceny bezpieczeństwa oraz do uzyskiwania i wydawania spójnych standardowych autoryzacji dla agencji rządowych w celu korzystania z ofert zatwierdzonych dostawców usług w chmurze.

4. Standardy ciągłego monitorowania, które wymagają określonych, standardowych działań w ramach „Bieżącej oceny i autoryzacji", które obejmują bieżącą, okresową ponowną ocenę systemów dostawcy usług w chmurze w celu potwierdzenia zgodności z wymogami bezpieczeństwa FedRAMP, w celu potwierdzenia, że wymagane środki kontroli bezpieczeństwa są nadal skuteczne, a zatem zachować bieżące zezwolenie.

5. Listy autoryzowanych usług, które identyfikują dostawców usług w chmurze, którzy uzyskali certyfikat „Upoważnienia do działania" wydany przez agencję rządową udzielającą zezwolenia lub certyfikat „Tymczasowego upoważnienia do działania" wydany przez Wspólną Radę Autoryzacyjną FedRAMP i w związku z tym są dostępni do użytku przez dowolny rząd agencja. (Listy autoryzowanych dostawców usług w chmurze są dostępne na Stronie internetowej GSA).

Wymagania bezpieczeństwa FedRAMP, którym muszą sprostać dostawcy usług w chmurze, są zgodne z FISMA. Opierają się one na kontrolach bezpieczeństwa wymienionych w publikacji specjalnej NITS

800-53, wersja 3, która dodaje kontrole bezpieczeństwa zorientowane na chmurę, których nie ma we wcześniejszych wersjach tego standardu. Oceny bezpieczeństwa FedRAMP dodają dodatkowe kontrole do ocen FedRAMP, które nie są uwzględnione w ocenach FISMA. Oceny FedRAMP są inicjowane przez poszczególnych dostawców usług w chmurze lub przez agencje rządowe, które chcą korzystać z usług w chmurze. Dostawca usług w chmurze (lub agencja rządowa zainteresowana uzyskaniem usług w chmurze) zatrudnia akredytowaną przez FedRAMP, komercyjną zewnętrzną organizację oceny bezpieczeństwa, tak zwaną organizację oceny trzeciej strony (3PAO). 3PAO używają standardów FedRAMP:

(a) Opracowanie planu oceny bezpieczeństwa, który jest specyficzny dla dostawcy usług w chmurze, który ma zostać poddany ocenie, i który określa środki kontroli bezpieczeństwa, które mają zostać ocenione, sposób wdrażania środków kontroli w środowisku dostawcy usług w chmurze, zasady zachowania w zakresie bezpieczeństwa i prywatności, granice środowiska dostawcy usług w chmurze oraz innych planów związanych z bezpieczeństwem,

(b) Przeprowadzenie oceny bezpieczeństwa środków kontroli bezpieczeństwa dostawcy usług w chmurze w celu określenia skuteczności wdrożeń wszystkich środków kontroli bezpieczeństwa określonych w planie oceny bezpieczeństwa oraz

(c) Opracowanie raportu z oceny bezpieczeństwa, który zostanie przedłożony do zatwierdzenia przez ocenianego dostawcę usług w chmurze. W razie potrzeby dostawca usług w chmurze opracuje i zrealizuje plan korygowania wszelkich słabych punktów lub wad stwierdzonych podczas oceny bezpieczeństwa 3PAO. Jeśli autoryzacja zostanie przyznana, wówczas zgodnie ze standardem ciągłego monitorowania FedRAMP, 3PAO może przeprowadzać coroczną, uzupełniającą, ponowną ocenę bezpieczeństwa systemów dostawcy usług w chmurze, aby dostawca usług w chmurze zachował autoryzację FedRAMP do dalszego używania przez agencje rządowe jako zatwierdzony dostawca usług w chmurze. Strony, które chcą zostać 3PAO FedRAMP, muszą przejść rygorystyczną ocenę zgodnie ze standardowymi kryteriami jakości i akceptowalności FedRAMP stosowanymi w celu zapewnienia kompetencji oceny bezpieczeństwa 3PAO, jak również zgodności procesów oceny bezpieczeństwa 3PAO. Aby wykorzystać korzyści płynące z korzystania z ocenionego i autoryzowanego dostawcy usług w chmurze, zachęca się agencje rządowe do wymagania w umowie, aby ich potencjalny dostawca usług w chmurze spełniał wymagania bezpieczeństwa FedRAMP. Dostępne są szczegółowe informacje na temat FedRAMP, jej procesów i wskazówek, jak korzystać z procesów FedRAMP. Aby być obserwowanym, Cloud Security Alliance rozważa wykorzystanie Open Certification Framework (OCF) oraz Security, Trust & Assurance Registry (STAR) wysiłków w celu opracowania czegoś, co wydaje się być międzynarodową wersją oceny i certyfikacji dostawców usług w chmurze w stylu FedRAMP.

Wspólne kryteria

Z doświadczeń zebranych w Orange Book i innych kryteriów krajowych, pojawiła się nowa, napędzana komercyjnie, standardowa strategia testowania produktów i wykazania pewności, że ich zabezpieczenia działają właściwie. Ta najlepsza ze wszystkich dotychczasowych strategii opiera się na międzynarodowym standardzie ISO 15408, Common Criteria for Information Technology Security Evaluation, zwanym potocznie Common Criteria (CC). Strategia CC oferuje jeden, uznane na całym świecie, podejście do specyfikacji wymagań bezpieczeństwa konsumentów oraz do komercyjnej oceny bezpieczeństwa produktów IT. Produkty mogą być budowane w dowolnym kraju, oceniane w dowolnym innym kraju i kupowane bez obaw w jeszcze innym kraju. To podejście CC jest przydatne w kilku społecznościach międzynarodowych. W Stanach Zjednoczonych jest akceptowany przez sektor rynkowy DoD i inne społeczności, takie jak sektor finansowy. Paradygmat CC przedstawia standardową strategię, która przezwycięża wady innych podejść. Zapewnia standardowy sposób określania (1)

budzących obawy zagrożeń, (2) wymagań funkcjonalnych bezpieczeństwa, które należy spełnić, aby złagodzić określone zagrożenia, oraz (3) wymagań zapewnienia bezpieczeństwa, które należy spełnić, aby zapewnić pewność, że produkty są zbudowane z pożądaną jakością. Zapewnia uznany, niezawodny i utrzymywany mechanizm budowania zaufania, który:

1. Wymagania bezpieczeństwa są poprawnie określone,

2. Sprzedawcy nie rozumieją źle wymagań i

3. Dostawcy projektują i wytwarzają produkty spełniające wymagania i zapewniające integralność ryzyka.

CC zapewnia elastyczny proces określania i testowania wymagań bezpieczeństwa dla wszystkich klas i konkretnych instancji wszystkich istniejących lub przyszłych produktów IT. W paradygmacie CC ryzyka i wymogi ochrony konsumentów są tak określone, aby rozwiązania bezpieczeństwa producentów produktów mogły zostać przetestowane (w standardowy sposób), aby móc zweryfikować (w standardowy sposób) zgodność produktu z określonymi standardowymi wymaganiami bezpieczeństwa. Badanie jest wykonywane przez jedno z laboratoriów badawczych, które posiadają akredytację (w standardowy sposób). W przeciwieństwie do innych podejść, CC zapewnia sposób na określenie wymagań dotyczących pewności i ocenę, w jakim stopniu są one spełnione. Wymogi dotyczące pewności są niezwykle ważne i zwykle nie są uwzględniane w innych podejściach do oceny produktów. Wymogi dotyczące pewności są podstawowymi składnikami budowania zaufania do wdrażania zabezpieczeń oraz zapewniania poziomu zaufania niezbędnego dla gospodarek i rządów, aby polegać na nowych modelach e-biznesu i e-administracji. Zaufanie do produktów buduje się poprzez zdobycie pewności, że funkcje bezpieczeństwa, które rzekomo zostały wdrożone w celu spełnienia określonych wymagań funkcjonalnych bezpieczeństwa (1) skutecznie spełniają określone cele bezpieczeństwa oraz (2) są wdrożone poprawnie i całkowicie oraz działają zgodnie z oczekiwaniami. Dzięki wymogom zapewnienia bezpieczeństwa zaufanie jest dalej umacniane poprzez zapewnienie, że twórcy produktów mają solidne procesy i podejmują określone działania w celu zapewnienia określonej jakości przez cały cykl życia produktu, który tworzą, testują, dostarczają i utrzymują. CC ustanawia również standardową metodę opracowywania wspólnych testów i metod oceny oraz wykorzystywania ich do weryfikacji aspektów bezpieczeństwa produktów za pośrednictwem kompetentnych, akredytowanych laboratoriów. Testy oparte na CC pomagają producentom obniżyć koszty, udostępniając pulę prywatnych, licencjonowanych, konkurencyjnych laboratoriów testujących zabezpieczenia, które mają spójną, akredytowaną jakość i kompetencje w zakresie testowania. Ponieważ testowanie jest standaryzowane i uznawane na całym świecie, koszty testowania są w efekcie ograniczone, ponieważ sprzedawcom produktów oszczędza się kosztownych kampanii ponownego testowania w poszczególnych krajach lub klientach. Oceny produktów składają się zarówno z analizy, jak i testowania produktu. Stosowanie standardowych kryteriów oceny i standardowej metodologii oceny prowadzi do powtarzalnych, obiektywnych wyników testów i ocen. Aby zaradzić wykrytym podczas oceny niedociągnięciom i wadom produktów, laboratoria testujące CC przekazują wyniki testów dostawcom produktów i współpracują w celu usunięcia wykrytych wad i niedociągnięć. Niezależny przegląd i walidacja testów i ocen opartych na CC przez akredytowane krajowe organy walidacyjne CC jeszcze bardziej zwiększają zaufanie konsumentów. Takie jednostki walidujące CC weryfikują wyniki testów i poświadczają, że produkty zostały pomyślnie ocenione zgodnie ze standardowymi testami i oceną przeprowadzoną przez akredytowane laboratoria testujące CC. Organy te są również odpowiedzialne za utrzymanie infrastruktury testowania i oceny bezpieczeństwa narodowego, która obejmuje (a) prawidłowe, spójne, wiarygodne, kompetentne i komercyjne stosowanie standardów i metod CC przez akredytowane laboratoria testujące CC w ich kraju, (b) rządowy organ nadzoru oraz c) rządowy organ wydający certyfikat oceny bezpieczeństwa.

Specyfikacja CC i podejście do testowania można w równym stopniu zastosować do wszystkich rodzajów produktów związanych z bezpieczeństwem, takich jak:

(a) Produkty, które wdrażają technologie bezpieczeństwa (np. kryptografy, systemy wykrywania/zapobiegania włamaniom, urządzenia i systemy ochrony granic, narzędzia audytowe, urządzenia kontroli dostępu, produkty do podpisu cyfrowego i wiele innych),

lub

(c) Produkty wspierające bezpieczeństwo (np. systemy operacyjne, systemy zarządzania certyfikatami, systemy zarządzania siecią, karty inteligentne i inne).

Stale rosnąca lista tysięcy produktów, które zostały ocenione zgodnie ze standardowymi testami opartymi na CC i które otrzymały certyfikaty CC, jest dostępna online75. Krótko mówiąc, paradygmat CC powiększa pulę lepiej zaprojektowanych, bardziej akceptowalnych produktów. Gdy certyfikowane produkty są zmieniane lub aktualizowane, dostawcy takich produktów mogą realizować standardowy proces utrzymania gwarancji w celu utrzymania poziomu gwarancji związanego z pierwotną certyfikacją takich produktów. Informacje o tym procesie pojawiają się gdzie indziej. CC to współczesny ujednolicony wybór służący budowaniu zaufania do produktów. Stosowanie norm ma tendencję do zwiększania atrakcyjności produktu dla różnych niezwiązanych ze sobą grup konsumentów. Kultura bezpieczeństwa konstruktora produktu ulega znacznej poprawie ze względu na wymaganą weryfikację skrupulatnego i wyraźnego skupienia się konstruktora na bezpieczeństwie, a także dyscyplin projektowania zabezpieczeń, opracowywania, testowania i konserwacji. Taka poprawa kultury zwykle przynosi korzyści innym produktom zbudowanym przez dostawcę. Niektórzy — szczególnie zwolennicy paradygmatu 20 krytycznych kontroli - wydają się uważać, że podejście CC jest zbyt elastyczne, wymaga zbyt dużej wiedzy specjalistycznej, aby wykorzystać jego elastyczność i byłoby lepiej, gdyby określało mały, obowiązkowy zestaw „zdroworozsądkowej" kontroli wartości w „większości" sytuacji. Z drugiej strony szanowane firmy konsultingowe doszły do wniosku, że ocena CC zapewnia znaczną poprawę w stosunku do niestandardowych lub nieformalnych metod testowania, które zazwyczaj skutkują poważnym niedostatecznym przetestowaniem oprogramowania i które jako grupa niespójnych podejść zapewniają jedynie porównania typu „jabłka do pomarańczy". testowanych produktów. Paradygmat CC zapewnia dodatkowy poziom należytej staranności. Poprawia i różnicuje produkty oraz umożliwia kupującym obiektywne porównywanie produktów. Jest akceptowany za obopólną zgodą w większości największych na świecie krajów rozwijających się i kupujących IT.

Przegląd paradygmatu wspólnych kryteriów

Paradygmat CC wykorzystuje międzynarodowe standardy, procesy i procedury do określania, testowania, walidacji i certyfikacji produktów związanych z bezpieczeństwem. Paradygmat CC to wielozadaniowy schemat dla:

* Określenie wymogów bezpieczeństwa, które mogą być stosowane przy zakupach produktów,

* Określanie towarzyszących rozwiązań bezpieczeństwa w produktach,

* Testowanie produktów zgodnie z dostosowanymi do produktu — ale standardowymi — kryteriami i metodologiami testowania przy użyciu akredytowanych, zewnętrznych, komercyjnych laboratoriów badawczych,

* Niezależne sprawdzanie poprawności wyników testów i

* Dostarczanie certyfikatów przetestowanym i zatwierdzonym produktom, które eliminują potrzebę dalszego ponownego testowania produktów dla różnych grup konsumenckich lub we wszystkich krajach, które wzajemnie uznają możliwości testowania komercyjnego i wyniki testów.

Konsumenci stosują standardową metodologię, standardowy język i katalog standardowych wymogów bezpieczeństwa w celu opracowania profili bezpieczeństwa (zob. sekcja 51.5.3.3) dostosowanych do rodzajów produktów, które chcą kupić. Profile określają potrzeby funkcjonalne bezpieczeństwa. Wymagają one również zaufania lub gwarancji pożądanej w produktach, jak również w procesach konstruktorów produktów, od projektowania produktu po konserwację. Konstruktorzy produktów wykorzystują tę samą standardową metodologię, język i katalog do opracowywania różnych typów profili bezpieczeństwa (patrz sekcja 51.5.3.4) w celu zdefiniowania specyfikacji bezpieczeństwa swoich produktów. Definiują specyfikacje bezpieczeństwa produktu pod względem zarówno funkcjonalności bezpieczeństwa, jak i zapewnienia bezpieczeństwa produktu i procesów konstruktorów. Specyfikacje konstruktorów pokazują, w jaki sposób ich produkty spełniają deklarowane potrzeby w zakresie bezpieczeństwa i bezpieczeństwa konsumentów. Specyfikacje producentów mogą również pokazywać, w jaki sposób ich produkty spełniają wszelkie dodatkowe funkcje bezpieczeństwa deklarowane przez producentów, które wykraczają poza deklarowane potrzeby konsumentów.

Elementy specyfikacji paradygmatu CC

Standard CC definiuje używany w nim język, metodologie stosowane do konstruowania i struktury dla dwóch typów profili bezpieczeństwa, które określają wymagania bezpieczeństwa: profile ochrony (PP) i cele bezpieczeństwa (ST). PP pomagają konsumentom określić, jakie zagrożenia i słabe punkty są ważne, podczas gdy ST pomagają sprzedawcom określić, jakie zagrożenia i słabe punkty są eliminowane przez ich produkty. PP pomagają konsumentom wyrazić, jakiego poziomu ochrony i zaufania oczekują od produktów, podczas gdy ST pomagają sprzedawcom określić, jaki poziom ochrony i zaufania zapewniają ich produkty. PP zapewniają standardowy i elastyczny sposób przekształcania potrzeb i zasad bezpieczeństwa konsumentów w jednoznaczne, neutralne dla produktu wymagania bezpieczeństwa dla pożądanego zachowania bezpieczeństwa i jakości dla dowolnej klasy produktów IT. Te dwa typy profili obejmują zarówno wymagania funkcjonalne bezpieczeństwa, jak i wymagania pewności. Wymagania funkcjonalne określają pożądane zachowanie bezpieczeństwa i są pobierane ze standardowego katalogu CC zawierającego setki takich wymagań. Wymogi dotyczące pewności stanowią podstawę do budowania zaufania poprzez nałożenie ograniczeń na to, jak dobrze zbudowany jest produkt lub profil. Wymagania dotyczące pewności są również skatalogowane w standardzie CC jako wymagania dotyczące, na przykład, (a) zarządzania konfiguracją produktu, (b) projektowania, opracowywania, dostarczania i eksploatacji produktu, (c) utrzymywania pewności przez cały okres użytkowania produktu cyklu życia i (d) znacznie więcej. Wymagania dotyczące pewności są zebrane w siedem standardowych, predefiniowanych pakietów zwanych poziomami pewności oceny (EAL). Pakiety o wyższym poziomie pewności (np. EAL4) zawierają bardziej rygorystyczne wymagania dotyczące pewności wymagające bardziej rygorystycznego metodologicznie projektowania i testowania niż pakiety niższego poziomu podstawowego (np. EAL1), które wymagają jedynie testów funkcjonalnych. EAL są wyliczane w monotonicznie rosnącej skali, która równoważy (a) rosnące poziomy ufności, które można uzyskać, z (b) rosnącymi kosztami i malejącą wykonalnością przeprowadzenia testów i oceny niezbędnych do wypracowania określonego, wyższego poziomu ufności. Im wyższy poziom pewności, tym więcej aspektów procesu rozwoju dostawcy będzie musiało zostać zbadanych podczas testowania i oceny produktu. Z najniższej półki, EAL1 może służyć na przykład do potwierdzenia twierdzenia, że dochowano należytej staranności w odniesieniu do ochrony danych osobowych oraz do ustalenia minimalnego stopnia pewności co do prawidłowego działania produktu w środowisku, w którym zagrożenia bezpieczeństwa nie są uważane za bardzo poważne. W

skrajnym przypadku EAL7 wymaga formalnie zweryfikowanego projektu i obszernej analizy formalnej. EAL7 może mieć zastosowanie do niektórych bardzo specyficznych, być może jedynych w swoim rodzaju produktów, przeznaczonych do sytuacji skrajnie wysokiego ryzyka lub tam, gdzie wysoka wartość chronionych aktywów uzasadnia nadzwyczajne koszty oceny do tego poziomu pewności. Typowe produkty handlowe mieszczą się w zakresie od EAL1 do EAL4. Podczas określania wymagań dotyczących pewności, pożądany poziom pewności – i koszt uzyskania takiej pewności – powinien być wyważony w stosunku do czynników, takich jak (1) wartość zasobów, które mają być chronione, (2) ryzyko i zakres możliwych strat, (3) pożądany poziom pewności oraz (4) wszelkie racjonalnie oczekiwane czynniki kosztów i opóźnień, które mogą towarzyszyć rozwojowi oraz wszelkim późniejszym testom, ocenie i walidacji produktu na określonym poziomie pewności. Podczas gdy PP określa ogólne, neutralne dla produktu wymagania dotyczące funkcjonalności i zapewnienia bezpieczeństwa dla określonej klasy produktów informatycznych, które spełniają potrzeby potencjalnych nabywców, ST jest specyficznym dla produktu postanowieniem dotyczącym wymagań dotyczących funkcjonalności i zapewnienia bezpieczeństwa, które obejmuje jeden, konkretnego produktu wraz z informacją, w jaki sposób wdrożony produkt spełnia określone wymagania bezpieczeństwa. Zgodnie z załączonym ST, określony produkt może deklarować zgodność z jednym lub większą liczbą PP, jak również z dodatkowymi wymaganiami dotyczącymi bezpieczeństwa produktu wymienionymi w jego ST. Biorąc pod uwagę zakres, głębokość i zmienność możliwych wymagań bezpieczeństwa, które można określić w PP lub ST, CC zapewnia możliwość określenia wymagań użytkownika i wymagań produktowych praktycznie nieograniczonej liczby istniejących i dopiero powstających konsumentów potrzeby bezpieczeństwa (PP) i rozwiązania w zakresie produktów bezpieczeństwa (ST). Celem testowania i oceny produktu w oparciu o CC jest ocena i potwierdzenie, że produkt spełnia specyficzne wymagania produktu i kryteria oceny zawarte w ST produktu. Wymagania ST dotyczące pewności mają wpływ na wymaganą głębokość i zakres testowania i oceny. Wiele produktów, które przeszły pomyślnie testy i oceny, pójdzie dalej, a ich wyniki testów i ocen zostaną zatwierdzone przez formalną, uznaną, krajową jednostkę walidacyjną CC. Produkty mogą następnie zostać certyfikowane przez rządowy organ wydający certyfikaty i dodane do publicznie dostępnego repozytorium zawierającego listę produktów z certyfikatem CC.

Konstruowanie profili ochrony

PP wyliczają potrzeby konsumentów w zakresie funkcjonalności i zapewnienia bezpieczeństwa, które są odpowiednie i wartościowe dla określonego typu produktu w celu złagodzenia określonych zagrożeń w określonym środowisku zagrożeń. Każdy PP określa problem bezpieczeństwa, który ma rozwiązać produkt zgodny z PP. Określa wymagania funkcjonalne bezpieczeństwa, o których wiadomo, że są przydatne i skuteczne w spełnianiu określonych celów bezpieczeństwa. Określa również wymagania dotyczące zapewnienia bezpieczeństwa, które zapewniają pożądaną pewność, że produkty są zbudowane z pożądaną jakością. Główna treść PP obejmuje stwierdzenia dotyczące:

1. Zagrożenia i Podatności, na które produkt będzie narażony,

2. Środowisko bezpieczeństwa, w którym produkt ma się znajdować, w tym (a) opisy zarówno informatycznych, jak i pozainformatycznych aspektów środowiska, (b) założenia dotyczące użytkowania, administrowania i zarządzania produktem oraz (c) wszystkie polityki , prawa, przepisy i zasady, z którymi produkt musi być zgodny w zamierzonym środowisku,

3. Cele bezpieczeństwa, jakie ma spełniać produkt lub środowisko, w którym produkt działa, w tym opisy zagrożeń i polityk, które mają być eliminowane przez produkt, a które mają być eliminowane przez środowisko,

4. Wymagania bezpieczeństwa, zarówno funkcjonalne, jak i zapewnienia bezpieczeństwa, wybrane i udoskonalone ze standardowych katalogów wymagań CC, aby spełnić każdy cel i założenie bezpieczeństwa, wskazujące, które wymagania są adresowane przez produkt, a które przez środowisko, w którym działa, oraz

5. Przedstawione uzasadnienie uzasadniające wszystkie decyzje i wybory dokonane podczas opracowywania treści w ramach PP. Uzasadnienie zawiera stwierdzenia, takie jak to, w jaki sposób wybrane wymagania bezpieczeństwa są odpowiednie do przeciwdziałania wyliczonym zagrożeniom, w jaki sposób są one zgodne z wyliczonymi zasadami i założeniami oraz w jaki sposób odwzorowują pierwotne, podstawowe, napędzające potrzeby i zagrożenia. Dostępne są wytyczne dotyczące opracowywania PP.78 Lista PP, które zostały formalnie zatwierdzone pod kątem poprawności, jest utrzymywana na stronie internetowej CC.

Konstruowanie profili docelowych zabezpieczeń

Twórcy produktów tworzą ST w celu udokumentowania szczegółowych informacji o aspektach bezpieczeństwa tworzonych przez nich produktów oraz określenia, w jaki sposób zaimplementowane funkcje bezpieczeństwa i środki bezpieczeństwa spełniają potrzeby konsumentów. ST zapewnia podstawę i kryteria oceny, według których przeprowadzane są testy i ocena produktu. Określa również konfigurację, w jakiej produkt ma być przetestowany. Zawartość ST jest podobna do PP. ST opisuje środowisko, w którym ma działać produkt opisany przez ST. ST wymienia (a) zagrożenia dla produktu, (b) zasady, prawa i przepisy, z którymi produkt ma być zgodny, oraz (c) założenia dotyczące aspektów bezpieczeństwa środowiska informatycznego i pozainformatycznego, w którym produkt jest przeznaczony do użytku. ST określają cele bezpieczeństwa, do których odnosi się twórca określonego produktu. ST wymieniają również wymagania bezpieczeństwa, które producent produktu spełnia, jak również te wymagania, które ma spełnić środowisko, w którym produkt ma działać. Niektóre z tych wymagań mogą być udoskonaleniami ogólnych lub neutralnych dla produktu wymagań określonych w PP, do których ST deklaruje zgodność; a niektóre mogą stanowić dodatkowe wymagania dotyczące bezpieczeństwa wykraczające poza te określone w PP, z którymi produkt ma być zgodny. ST wykracza jednak poza PP, ponieważ określa również funkcje bezpieczeństwa oferowane przez produkt w celu spełnienia każdego z wymagań bezpieczeństwa określonych w ST. Określa również środki zapewnienia bezpieczeństwa podjęte przez konstruktora produktu w celu spełnienia wszystkich wymagań bezpieczeństwa określonych w ST. Przedstawiono również uzasadnienie wszystkich decyzji i wyborów dokonanych podczas opracowywania treści ST. Uzasadnienie uzasadnia wszystkie twierdzenia zawarte w ST dotyczące PP, z którymi produkt jest zgodny. Zasadniczo przedstawione uzasadnienie pokazuje, że ST zawiera skuteczny i odpowiedni zestaw środków zaradczych oraz że ten zestaw środków zaradczych jest spójny, kompletny i spójny. Porównując ST różnych produktów, konsumenci są w stanie lepiej porównać zabezpieczenia konkurencyjnych produktów. Konsumenci są w stanie zrozumieć, jakiego rodzaju testom i ocenom został poddany konkretny produkt. Są również w stanie określić, czy konfiguracja, w której produkt był testowany, jest zgodna ze środowiskiem, w którym produkt zostanie wdrożony.

Wspólne testowanie produktów

Produkty charakteryzujące się powiązanymi specyficznymi dla produktu ST mogą być poddawane standardowym testom i ocenie CC przy użyciu standardowej metodologii przez dowolne oficjalnie akredytowane/licencjonowane laboratorium testujące i oceniające CC w dowolnym miejscu na świecie. Testy zapewniają, że produkty są poprawne, kompletne, dobrze zbudowane i zgodne ze specyfikacjami bezpieczeństwa. Testy przeprowadza się w warunkach odpowiednich do zamierzonej normalnej pracy produktu, tak aby zweryfikować, czy zastosowane zabezpieczenia są prawidłowe,

kompletne i zgodne w normalnych warunkach eksploatacji. Ponieważ testowanie oparte na CC może wykazać identyfikowalność aspektów bezpieczeństwa produktu z wymaganiami użytkownika produktu, a także z obowiązującymi zasadami, prawami i regulacjami, takie testy mogą zmniejszyć narażenie użytkowników produktu na potencjalne kary za nieprzestrzeganie zasad związanych z bezpieczeństwem prawa lub przepisy. Laboratoria badawcze i ich personel są akredytowani ze względu na swoje kompetencje w zakresie oceny bezpieczeństwa, jak określono w rozszerzeniu laboratorium badań bezpieczeństwa do normy ISO określającej ogólne wymagania dotyczące kompetencji laboratoriów badawczych. Zgodnie z definicją zawartą w standardzie CC Common Evaluation Methodology (CEM), ewaluatorzy stosują standardową metodologię z ustrukturyzowanymi, formalnymi procesami oceny i działaniami ewaluacyjnymi, aby przeprowadzić szereg standardowych działań testowych i ewaluacyjnych. Ponieważ testy są przeprowadzane zgodnie ze standardami, konsumenci mają silne poczucie, że testy są obiektywne i nie mają na celu przyniesienia korzyści testowanemu produktowi. Dzięki dodatkowemu zaufaniu, jakie stwarzają testy CC, klienci zmniejszają koszty zakupu produktów, minimalizując testy akceptacyjne, które powielają testy już przeprowadzone na produkcie przez akredytowane laboratorium testujące CC. Badania wskazują, że testy CC ulepszają produkty, eliminując możliwe do wykorzystania luki w zabezpieczeniach oraz dodając lub rozszerzając niezbędne funkcje bezpieczeństwa. Standard CEM zapewnia wspólną bazę dla niezależnych, autonomicznych laboratoriów testujących CC w celu oceny profili CC i produktów dostawców w ten sam sposób, niezależnie od używanego laboratorium testowego CC. Korzystanie z CEM przez wszystkie laboratoria testujące CC zapewnia wspólny poziom zaufania do podobnych produktów, które mogły zostać ocenione przez różne laboratoria testujące CC. Rzeczywiście, porozumienie o wspólnych kryteriach w sprawie wzajemnego uznawania certyfikatów wspólnych kryteriów w dziedzinie bezpieczeństwa technologii informatycznych, często nazywane po prostu porozumieniem o wzajemnym uznawaniu (MRA), jest wielonarodową deklaracją na poziomie traktatu, zgodnie z którą różne kraje będą uznawać CEM/ Oceny oparte na CC, które mogą być przeprowadzane przez laboratoria testujące CC w innych jurysdykcjach. Ponieważ CEM jest uznawany na całym świecie, stosowanie oceny unikalnej dla klienta lub kraju jest zminimalizowane, jeśli nie całkowicie unikane. Koszty oceny są zminimalizowane, ponieważ dostawcy muszą przygotować się tylko do jednej kampanii testowej, a nie do zestawu różnych kampanii testowych przeprowadzanych pod kątem różnych kryteriów oceny specyficznych dla klienta, firmy konsultingowej lub kraju. Chociaż niektórzy konsumenci i sprzedawcy uważają, że paradygmat CC jest skomplikowany, nieefektywny lub kosztowny, wielu, którzy tworzą i kupują zatwierdzone produkty, postrzega paradygmat CC jako najlepszy, proaktywny sposób na poprawę bezpieczeństwa i pewności produktów kupowanych i sprzedawanych w rynek.