tenable network security

SecurityCenter™ CV
continuous view

Stan zastany

W grudniu 2014 Komisja Nadzoru Finansowego opublikowała dokument „Wytyczne dotyczące zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w zakładach ubezpieczeń i zakładach reasekuracji". Dokument ten zawiera 22 wytyczne, które obligatoryjnie muszą być wdrożone do 31 grudnia 2016. Doświadczenie z wdrażania podobnych norm w sektorze bankowości (Rekomendacje D oraz M) uczy, że Komisja Nadzoru Finansowego nie będzie po zapadnięciu tego terminu stosowała taryfy ulgowej, tylko przystąpi do skrupulatnej weryfikacji wdrażania wytycznych.

Wytyczne opracowane przez KNF dotyczą czterech obszarów działania ubezpieczycieli:

- **strategii i organizacji obszarów technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego;**
- **rozwoju środowiska teleinformatycznego;**
- **utrzymania i eksploatacji środowiska teleinformatycznego;**
- **zarządzania bezpieczeństwem środowiska teleinformatycznego.**

Dodatkowo KNF przyjął zasadę, że wytyczne mają być stosowane wedle paradygmatu „zastosuj lub wyjaśnij". Oznacza to, że dane towarzystwo może odstąpić od stosowania niektórych wytycznych, ale organ nadzorczy oczekiwał wówczas będzie od takiego podmiotu szczegółowych wyjaśnień powodów, które uzasadniają nieuwzględnienie wytycznych w jego działalności. KNF będzie na bieżąco znał stan wdrożenia wytycznych w poszczególnych towarzystwach dzięki informacjom przekazywanym w ramach BION, co oznacza, że realizowane przezeń kontrole będą dobrze przygotowane i bardzo skuteczne.

Proponowane rozwiązanie

Należy realnie ocenić, że wypełnienie wymogów KNF bez wsparcia dedykowanych systemów informatycznych będzie zadaniem trudnym, długotrwałym, wymagającym alokacji znacznych sił i zasobów oraz potencjalnie obarczonym znacznym ryzykiem popełnienia błędów w szacowaniu oraz analizie. Dla tego też OpenBIZ Sp. z o.o. opracowało w oparciu o system Security Center Continous View rozwiązanie wspierające towarzystwa w zakresie pomiaru, analizy oraz raportowania dla poszczególnych wytycznych.

Poniżej przedstawiono wsparcie jakie może zapewnić oferowane rozwiązanie w poszczególnych obszarach wytycznych KNF.

System Security Center Continous View w sposób zautomatyzowany zbiera informacje o stanie bezpieczeństwa systemów, sieci oraz urządzeń działających w towarzystwie. Pozwala również na zbieranie informacji o zdarzeniach, które zaszły w monitorowanych systemach i korelowanie ich z informacjami o aktywności aplikacji i użytkowników. Trafne wdrożenie systemu Security Center Continous View zapewnia de facto wykonywanie pełnego, codziennego audytu wszystkich systemów towarzystwa. Można śmiało stwierdzić, że system Security Center Continous View jest dla rynku bezpieczeństwa teleinformatycznego tym, czym system SAP R/3 jest dla rynku ERP.

Oferta OpenBIZ Sp. z o.o. dla zakładów ubezpieczeń i asekuracji

Oferujemy kompleksowe rozwiązanie wdrożenia systemu nadzoru, analizy i raportowania wymogów stawianych przez wytyczne Komisji Nadzoru Finansowego. Jako autoryzowany partner producenta systemu, firmy Tenable Inc, oraz polskie centrum kompetencyjne, jesteśmy w stanie zapewnić pomoc w każdej fazie uruchamiania systemu, poczynając od analizy przedwdrożeniowej, poprzez wdrożenie, szkolenia i dostawę modułów zgodnych z wymogami KNF, a kończąc na umowie pełnego wsparcia w zakresie eksploatacji systemu w towarzystwie.

Security Center CV dla zakładów ubezpieczeń i zakładów asekuracyjnych

Rosnąca rola danych w gospodarce cyfrowej oraz rosnące zagrożenie ze strony cyberprzestępczości spowodowały zaostrzenie przez legislatorów wymogów dotyczących bezpieczeństwa.

Czytelność przekazywanych informacji

System Security Center Continous View przystosowany jest do pracy w organizacji posiadającej jasno określoną hierarchię, o dobrze zdefiniowanych zakresach kompetencji.

Zarząd i Rada nadzorcza

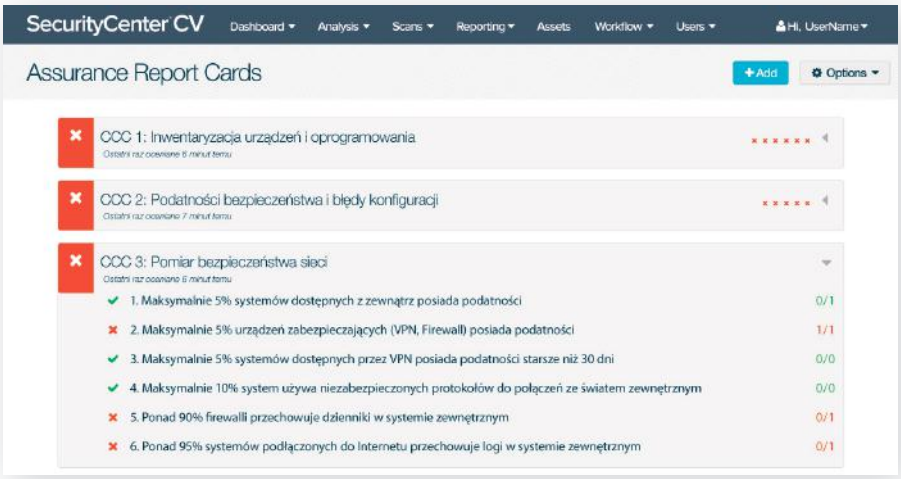
Na poziomie raportowania dla rady nadzorczej i zarządu system oferuje **karty realizacji celów strategicznych (Assurance Reports Cards)**, pozwalające w szybki sposób, bez wchodzenia w szczegóły techniczne, określić rzeczywisty poziom spełnienia wymogów poszczególnych wytycznych KNF. Pozwala to władzom towarzystwa na szybką i trafną ocenę stanu poziomu bezpieczeństwa, a co za tym idzie na podejmowanie decyzji dotyczących delegowania zadań lub konieczności podejmowania inwestycji w danym obszarze.

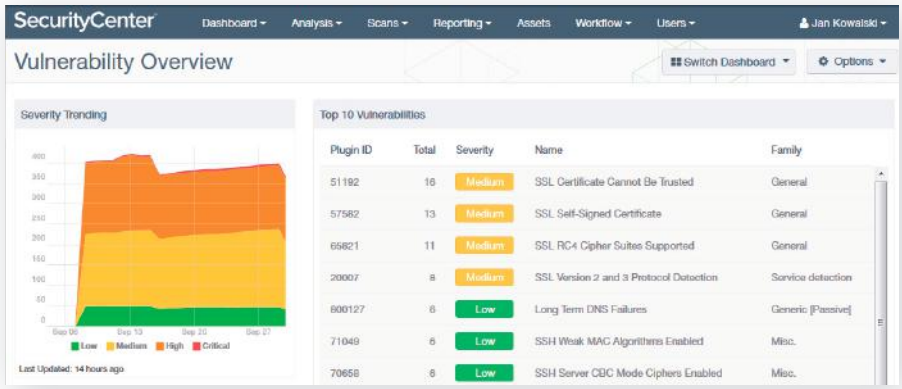
Szefostwo IT, pionu bezpieczeństwa oraz audytu wewnętrznego

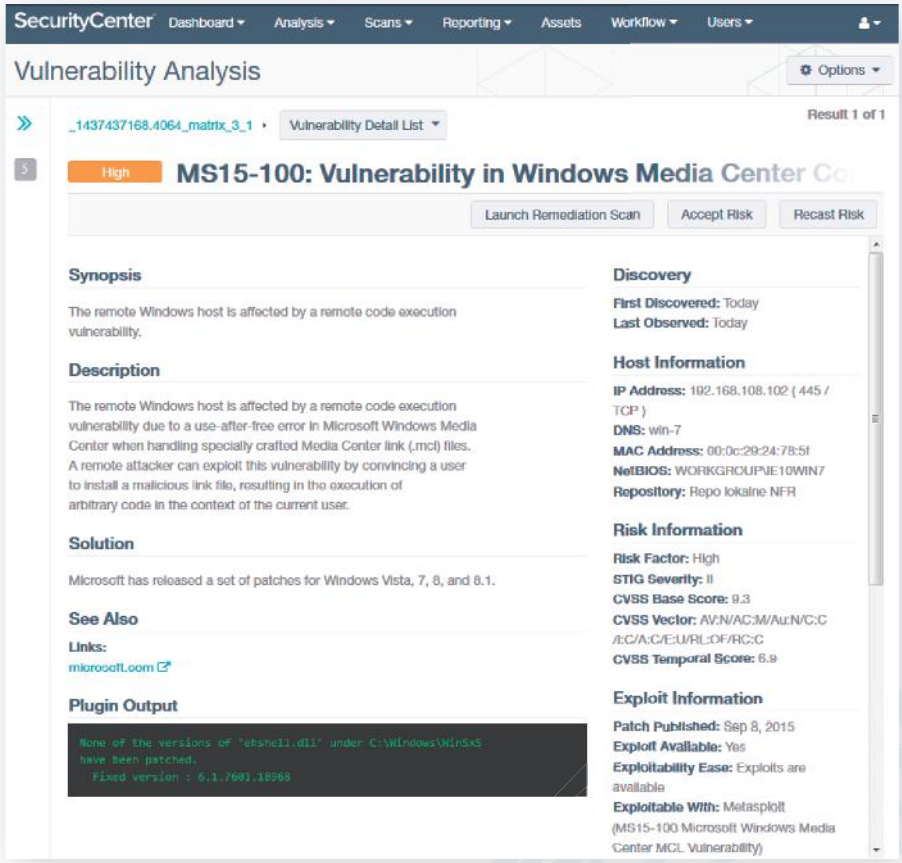
Na tym poziomie raportowania dostępne są informacje dotyczące konkretnych problemów istniejących w ramach obszarów wyznaczonych przez poszczególne wytyczne KNF. Pozwala to na trafne określenie: przyczyny powstania danego problemu, jego wpływu na działanie organizacji oraz środków zaradczych, które należy podjąć, wraz z jasnym określeniem zakresu odpowiedzialności. Na tym poziomie raportowania można również w łatwy sposób śledzić efektywność usuwania problemów i podatności przez służby IT lub zewnętrzne firmy działające na zasadzie outsourcingu.

Pracownicy IT, firmy outsourcingowe

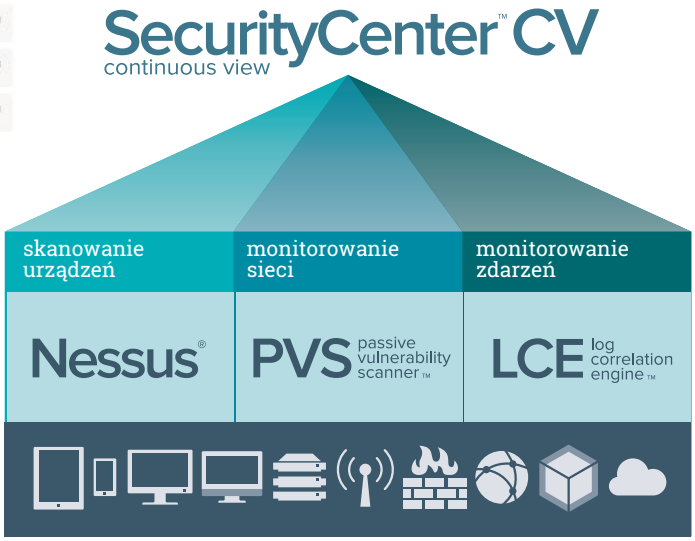
Na tym poziomie pracownicy otrzymują wykazy konkretnych problemów lub podatności bezpieczeństwa, które mają usunąć. Żelazną zasadą systemu Security Center Continous View jest, że każdy raport podatności zawsze zawiera informacje o sposobie jego usunięcia. Nie istnieje zatem ryzyko, że pracownik nie będzie wiedział jakie działania ma podjąć żeby rozwiązać dany problem.







Assurance Report Cards



Zarząd
całościowy pogląd

Managment
kontrola wykonania

Dział IT
wspomaganie wykonania

Dashboardy i raporty w czasie rzeczywistym

Zakres wytycznych KNF w odniesieniu do funkcjonalności Security Center Continous View

Wytyczna Komisji Nadzoru Finansowego	Security Center CV
I. Strategia i organizacja obszarów technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego	
Wytyczna 1. Rada nadzorcza towarzystwa powinna nadzorować funkcjonowanie obszarów technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego, natomiast zarząd towarzystwa powinien zapewnić, aby powyższe obszary zarządzane były w sposób poprawny i efektywny.	TAK
Wytyczna 2. W towarzystwie powinien funkcjonować sformalizowany system informacji zarządczej w zakresie obszarów technologii informacyjnej oraz bezpieczeństwa środowiska teleinformatycznego, zapewniający każdemu z odbiorców informacji właściwy poziom wiedzy o tych obszarach.	TAK
Wytyczna 3. Towarzystwo powinno opracować i wdrożyć strategię w zakresie obszarów technologii informacyjnej oraz bezpieczeństwa środowiska teleinformatycznego, zgodną ze strategią działania towarzystwa.	Pełne monitorowanie
Wytyczna 4. Towarzystwo powinno określić zasady współpracy oraz zakresy odpowiedzialności w obrębie obszaru biznesowego, technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego, pozwalające na efektywne i bezpieczne wykorzystanie potencjału środowiska teleinformatycznego w działalności towarzystwa.	TAK

Wytyczna Komisji Nadzoru Finansowego	Security Center CV
Wytyczna 5. Rozwiązania organizacyjne oraz zasoby ludzkie w obszarach technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego powinny być adekwatne do jego profilu ryzyka i specyfiki działalności oraz pozwalać na efektywną realizację działań w tych obszarach.	TAK
II. Rozwój środowiska teleinformatycznego	
Wytyczna 6. Towarzystwo powinno posiadać sformalizowane zasady prowadzenia projektów w zakresie środowiska teleinformatycznego, adekwatne do skali i specyfiki realizowanych projektów.	Pełne monitorowanie
Wytyczna 7. Systemy informatyczne towarzystwa powinny być rozwijane w sposób zapewniający wsparcie jego działalności oraz uwzględniający wymogi bezpieczeństwa środowiska teleinformatycznego	Pełne monitorowanie
III. Utrzymanie i eksploatacja środowiska teleinformatycznego	
Wytyczna 8. Towarzystwo powinno posiadać sformalizowane zasady zarządzania danymi wykorzystywanymi w ramach prowadzonej działalności (w tym danymi przetwarzanymi w hurtowniach danych), obejmujące w szczególności zarządzanie architekturą oraz jakością danych i zapewniające właściwe wsparcie działalności towarzystwa.	Pełne monitorowanie

Wytyczna Komisji Nadzoru Finansowego	Security Center CV
Wytyczna 9. Towarzystwo powinno posiadać sformalizowane zasady dotyczące zarządzania infrastrukturą teleinformatyczną wraz z systemami informatycznymi, w tym ich architekturą, poszczególnymi komponentami, wydajnością i pojemnością oraz dokumentacją, zapewniające właściwe wsparcie działalności towarzystwa oraz bezpieczeństwo przetwarzanych danych.	Pełne monitorowanie
Wytyczna 10. Towarzystwo powinno posiadać sformalizowane zasady współpracy z zewnętrznymi dostawcami usług informatycznych, zapewniające bezpieczeństwo danych i poprawność działania środowiska teleinformatycznego, uwzględniające również usługi świadczone przez podmioty należące do ubezpieczeniowej grupy kapitałowej.	Pełne monitorowanie
Wytyczna 11. Towarzystwo powinno posiadać sformalizowane zasady oraz mechanizmy techniczne zapewniające właściwy poziom kontroli dostępu logicznego do danych i informacji oraz dostępu fizycznego do kluczowych elementów infrastruktury teleinformatycznej.	Pełne monitorowanie
Wytyczna 12. Towarzystwo powinno zapewnić odpowiednią ochronę środowiska teleinformatycznego przed szkodliwym oprogramowaniem.	Pełne monitorowanie
Wytyczna 13. Towarzystwo powinno zapewniać wewnętrznym użytkownikom poszczególnych komponentów środowiska teleinformatycznego wsparcie w zakresie rozwiązywania problemów związanych z ich eksploatacją, w tym wynikających z wystąpienia awarii i innych niestandardowych zdarzeń zakłócających ich użytkowanie.	Częściowe monitorowanie
Wytyczna 14. Towarzystwo powinno podejmować skuteczne działania mające na celu osiągnięcie i utrzymanie odpowiedniego poziomu kwalifikacji pracowników w zakresie środowiska teleinformatycznego i bezpieczeństwa informacji przetwarzanych w tym środowisku.	NIE
Wytyczna 15. System zarządzania ciągłością działania towarzystwa powinien uwzględniać szczególne uwarunkowania związane z jego środowiskiem teleinformatycznym oraz przetwarzanymi w nim danymi.	Pełne monitorowanie
Wytyczna 16. Towarzystwo świadczące usługi z wykorzystaniem elektronicznych kanałów dostępu, w szczególności oferujące możliwość zarządzania produktami ubezpieczeniowymi z ubezpieczeniowym funduszem kapitałowym, powinno posiadać skuteczne rozwiązania techniczne i organizacyjne zapewniające weryfikację tożsamości i bezpieczeństwo danych oraz środków klientów, jak również edukować klientów w zakresie zasad bezpiecznego korzystania z tych kanałów.	Pełne monitorowanie

Wytyczna Komisji Nadzoru Finansowego	Security Center CV
Wytyczna 17. Towarzystwo powinno posiadać sformalizowane zasady zarządzania tzw. oprogramowaniem użytkownika końcowego, skutecznie ograniczające ryzyko związane z eksploatacją tego oprogramowania.	TAK
IV. Zarządzanie bezpieczeństwem środowiska teleinformatycznego	
Wytyczna 18. W towarzystwie powinien funkcjonować sformalizowany, skuteczny system zarządzania bezpieczeństwem środowiska teleinformatycznego, obejmujący działania związane z identyfikacją, mierzeniem, monitorowaniem, zarządzaniem i raportowaniem ryzyka w tym zakresie, zintegrowany z całościowym systemem zarządzania ryzykiem i bezpieczeństwem informacji w towarzystwie.	TAK
Wytyczna 19. Towarzystwo powinno klasyfikować systemy informatyczne i przetwarzane w nich informacje zgodnie z zasadami uwzględniającymi w szczególności wymagany dla tych systemów i informacji poziom bezpieczeństwa.	TAK
Wytyczna 20. Towarzystwo powinno posiadać sformalizowane zasady zarządzania incydentami naruszenia bezpieczeństwa środowiska teleinformatycznego, obejmujące ich identyfikację, rejestrowanie, analizę, priorytetyzację, wyszukiwanie powiązań, podejmowanie działań naprawczych oraz usuwanie przyczyn.	TAK
Wytyczna 21. Towarzystwo powinno zapewnić zgodność funkcjonowania obszarów technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego z otoczeniem prawnym, w tym regulacjami wewnętrznymi i zewnętrznymi, zawartymi umowami i przyjętymi w towarzystwie standardami oraz aktami nadzorczymi.	Pełne monitorowanie
Wytyczna 22. Obszary technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego powinny być przedmiotem systematycznych, niezależnych audytów.	TAK

OpenBIZ

Autoryzowany partner Tenable Inc.

OpenBIZ Sp. z o.o.
tel.: +48 22 350 67 95
+48 887 253 418
fax: +48 22 350 76 59
mail: openbiz@openbiz.pl