IT GRC – bezpieczeństwo IT skoncentrowane na ochronie biznesu organizacji

Jednym z największych wyzwań współczesnych organizacji jest zapewnienie należytej współpracy informatyki z obszarami biznesowymi. Bez tego nie jest możliwe stworzenie strategii bezpieczeństwa IT adekwatnej do rzeczywistych potrzeb organizacji ani racjonalne dysponowanie budżetem, jaki firma przeznacza na informatykę. Dużą pomoc w tym zakresie stanowią specjalistyczne rozwiązania IT GRC, czyli IT Governance, Risk management and Compliance, w Polsce jeszcze mało znane. Rozwiązanie IT GRC pozwala organizacjom na całościowe spojrzenie na bezpieczeństwo w obszarze technicznym i biznesowym oraz zautomatyzowanie najważniejszych procesów zarządzania bezpieczeństwem IT.

CZYM JEST IT GRC?

Na naszym rynku najbardziej znane rozwiązanie IT GRC to SecureVisio, stworzone przez polską firmę eSECURE. Rozwiązanie ma obecnie klientów w sektorach finansowym, rządowym i energetycznym. Podstawowym komponentem SecureVisio jest interaktywna, elektroniczna dokumentacja wyposażona w graficzne narzędzia do edycji, przeszukiwania i analizy danych istotnych dla bezpieczeństwa organizacji. Działalność firm coraz bardziej zależy od informatyki. Systemy IT wspomagają najważniejsze procesy biznesowe oraz przechowują i przetwarzają dane o krytycznym znaczeniu dla organizacji. Zakłócenie bezpieczeństwa systemów IT przekłada się bezpośrednio na zablokowanie lub zakłócenie działalności organizacji.

Polskie rozwiązanie IT GRC, eSECURE SecureVisio składa się z następujących, głównych komponentów:

- Elektroniczna dokumentacja zabezpieczeń z funkcjami automatyzacji pozyskiwania danych (m.in. skaner sieci, SNMP, SSH, WMI)
- Baza wiedzy eksperckiej bezpieczeństwa IT
- Specjalistyczne narzędzia:
  - Modelowanie zagrożeń
  - Audytowanie bezpieczeństwa
  - Szacowanie ryzyka
  - Ocena wpływu incydentu
  - Symulacja awarii
- Moduł integracji z SIEM, zabezpieczeniami sieci (FW, IPS, itp.), Vulnerability Assessment i bazą CVE®
- Moduł raportowania i alarmowania

Nie można efektywnie zarządzać bezpieczeństwem systemów IT bez posiadania kompletnej i aktualnej ich dokumentacji. Potrzebujemy informacji, które systemy IT wspomagają najważniejsze procesy organizacji, jak ważne dane są przez nie przetwarzane oraz jakie środki ochrony należy im zapewnić. W wielu organizacjach wiedza na ten temat znajduje się w głowach wielu ludzi i dziesiątkach dokumentów. Brak wiedzy prowadzi do błędów w planowaniu bezpieczeństwa, błędów w obsłudze incydentów i wynikających z tego strat dla organizacji oraz wielu stresujących sytuacji. Elektroniczna dokumentacja może zostać w razie potrzeby wyeksportowana do formy drukowalnej. Kreator generowania raportów umożliwia tworzenie dodatkowych dokumentów opisujących wybrane aspekty bezpieczeństwa wskazanych systemów IT. Elektroniczna dokumentacja i narzędzia SecureVisio umożliwiają łatwiejszą i efektywną kosztowo realizację złożonych projektów bezpieczeństwa, jak DLP i BCP. Narzędzia klasyfikacji i ustalania lokalizacji wrażliwych danych w systemie teleinformatycznym organizacji znacząco przyspieszają realizację i zwiększają prawdopodobieństwo sukcesu projektów DLP. Narzędzia automatyzujące proces Business Impact Analysis wspomagają realizację najtrudniejszego etapu projektu BCP, jakim jest ocena wpływu incydentów na działalność biznesową firmy.

UNIKANIE INCYDENTÓW W SYSTEMACH IT O KRYTYCZNYM ZNACZENIU DLA ORGANIZACJI

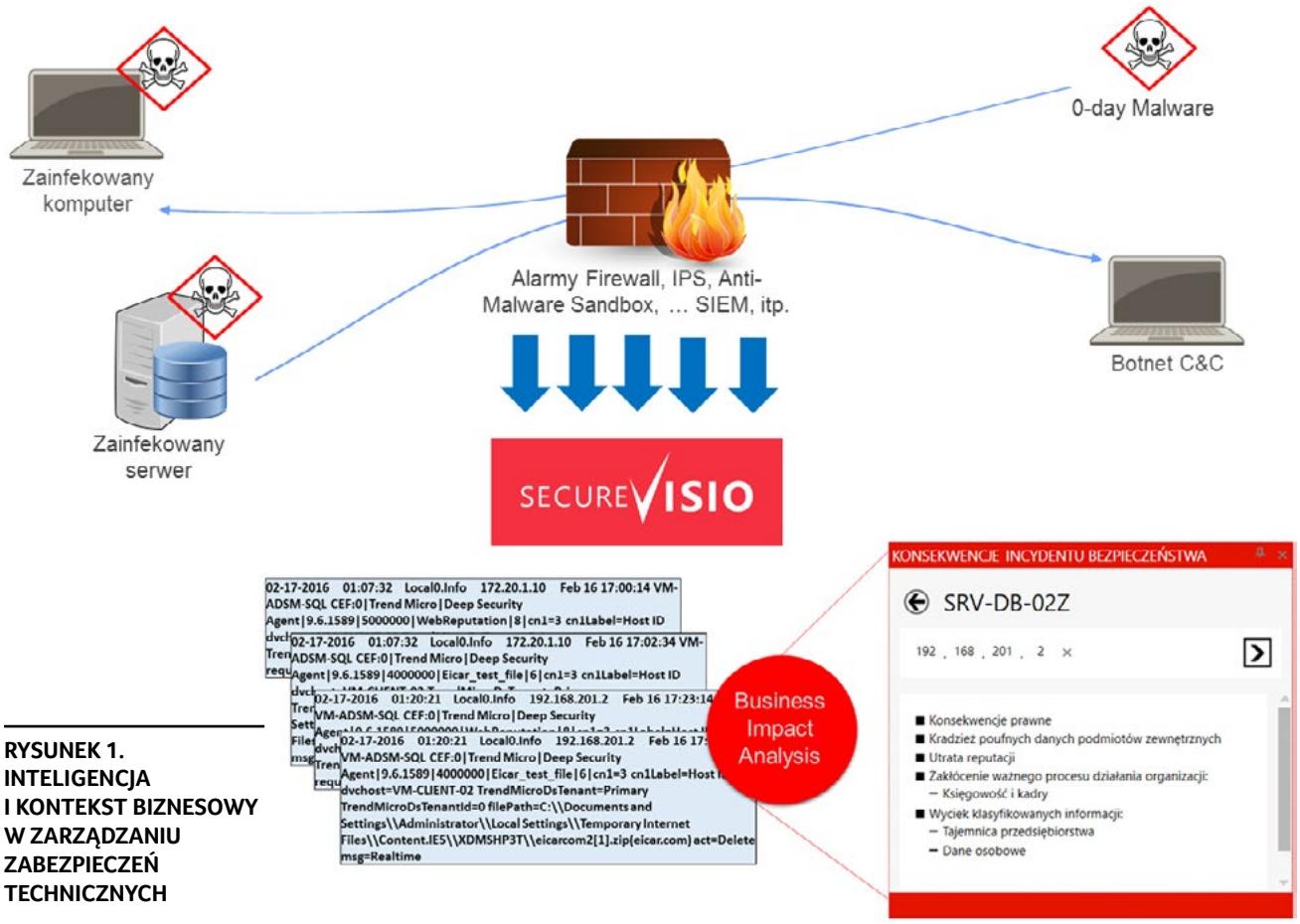
Dynamika zmian i pojawiające się każdego dnia nowe podatności w systemach IT sprawiają, że or-

ganizacje nie mogą uniknąć wszystkich incydentów bezpieczeństwa. Realistyczna strategia bezpieczeństwa zakłada, że powinny one przygotować się do szybkiego wykrywania incydentów i usuwania ich skutków (np. reinstalacji systemów, gdzie wykryto malware), zanim dojdzie do naruszeń bezpieczeństwa (np. kradzieży danych, zablokowania systemu). W całym obszarze systemu teleinformatycznego nie jest to możliwe. Dzięki IT GRC administratorzy bezpieczeństwa mogą skoncentrować uwagę na systemach IT najważniejszych dla organizacji i skutecznie obsługiwać incydenty tak, aby nie doszło tam do naruszeń bezpieczeństwa.

Zabezpieczenia techniczne (m.in. firewall, IPS, anti-malware sandbox) stanowią cenne źródło informacji nt. bezpieczeństwa systemów IT. Istotny problem w zarządzaniu bezpieczeństwem wynika z faktu, że zabezpieczenia techniczne generują bardzo dużą liczbę logów i alarmów, z których osobom odpowiedzialnym za bezpieczeństwo trudno jest „wyłowić" informacje rzeczywiście ważne dla działalności biznesowej organizacji. Systemy klasy SIEM operują w obszarze technicznym i same nie rozwiązują tego problemu. SecureVisio umożliwia automatyczną ocenę biznesowego znaczenia zdarzeń w systemie zabezpieczeń technicznych (np. alarmów firewall i IPS, alarmów SIEM) i dzięki temu szybkie wykrywanie incydentów w systemach IT ważnych dla organizacji zanim, dojdzie do naruszeń bezpieczeństwa (tj. zablokowania ważnych procesów biznesowych, wycieku poufnych danych, utraty reputacji i zaufania klientów).

WSPARCIE W PODEJMOWANIU TRUDNYCH DECYZJI

Mózgiem SecureVisio jest baza wiedzy eksperckiej, dzięki której odbywa się automatyczne modelowanie zagrożeń i audytowanie bezpieczeństwa. Baza wiedzy eksperckiej pełni rolę zespołu ekspertów z różnych obszarów bezpieczeństwa. SecureVisio utrzymuje zebrane przez ekspertów i regularnie aktualizowane informacje na temat różnych rodzajów systemów IT i ich podatności na różne rodzaje metod włamań i ataków, informacje na temat różnych rodzajów zabezpieczeń sieciowych i ich efektywności w przeciwdziałaniu różnym metodom włamań i atakom, informacje na temat efektywności ochrony zabezpieczeń lokalnych i wiele innych informacji istotnych w zarządzaniu bezpieczeństwem.



RYSUNEK 1. INTELIGENCJA I KONTEKST BIZNESOWY W ZARZĄDZANIU ZABEZPIECZEŃ TECHNICZNYCH

SecureVisio wyposażone jest w zestaw graficznych narzędzi wspomagających osoby odpowiedzialne za bezpieczeństwo IT, m.in.:

- Wyznacz źródła zagrożenia systemu IT
- Pokaż zabezpieczenia systemów IT przed potencjalnymi źródłami zagrożenia
- Pokaż najbardziej narażone systemy IT
- Pokaż lokalizację danych określonej kategorii
- Pokaż zakres i konsekwencje incydentu bezpieczeństwa
- Pokaż obszary sieci nie należące do organizacji
- Pokaż zabezpieczenia chroniące system przed określonym źródłem zagrożenia
- Pokaż lokalizację systemów określonego rodzaju
- Pokaż systemy posiadające określone zabezpieczenia lokalne
- Pokaż narzędzia zarządzania bezpieczeństwem dla urządzeń zabezpieczeń
- Pokaż narzędzia zarządzania bezpieczeństwem dla ważnych systemów IT
- Pokaż narażone systemy IT o krytycznym znaczeniu biznesowym
- Pokaż ważne systemy IT narażone na awarie (Single Point of Failure)
- Pokaż systemy IT o wysokim poziomie ryzyka
- Pokaż wielkość ryzyka systemów IT dla poszczególnych zagrożeń
- Pokaż niedziałające procesy biznesowe w sytuacji awarii określonego elementu systemów IT

EFEKTYWNE ZARZĄDZANIE PODATNOŚCIAMI W SKALI CAŁEJ ORGANIZACJI

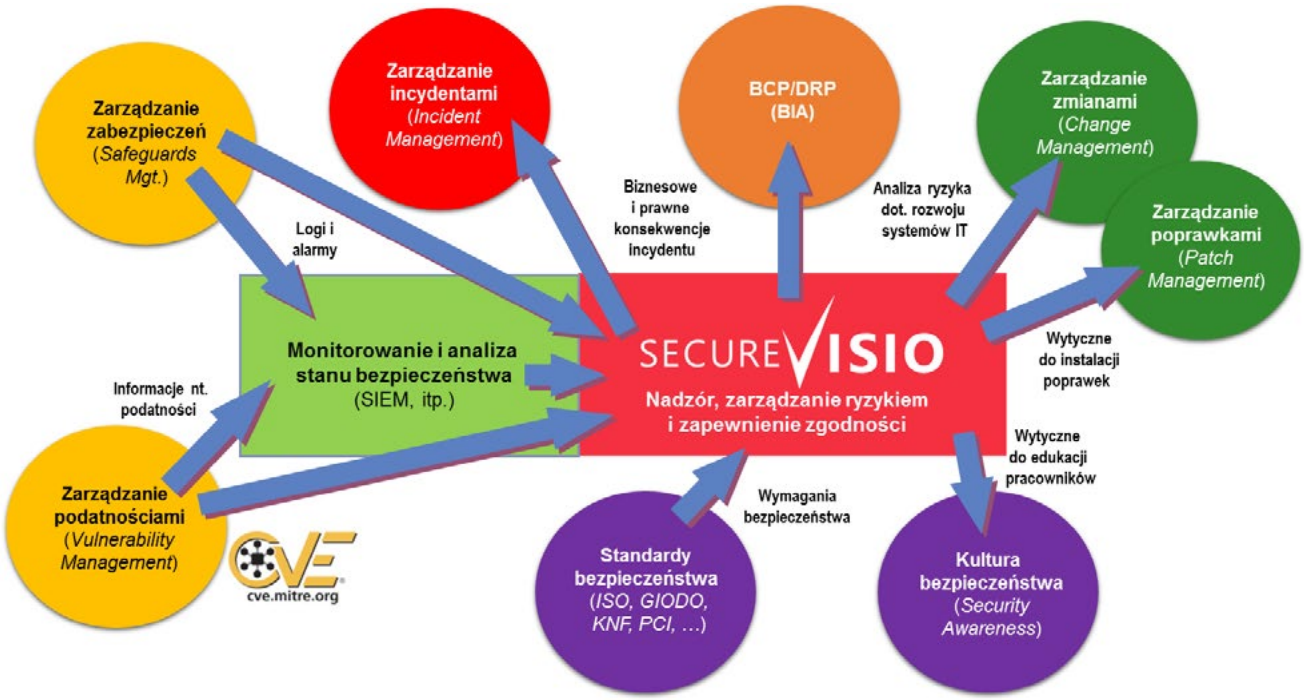
Trudność w utrzymaniu bezpieczeństwa IT polega na tym, że organizacje w praktyce nie mają możliwości usunięcia podatności wszystkich elementów systemów IT (m.in. błędów oprogramowania i konfiguracji systemów operacyjnych, aplikacji i baz danych). Realistyczna strategia bezpieczeństwa zakłada, iż należy szybko identyfikować i usuwać podatności w systemach IT o krytycznym znaczeniu dla firmy tak, aby nie dopuścić do wykorzystana ich przez intruzów i złośliwe programy.
Wykonując skanowanie sieci organizacji za pomocą narzędzi Vulnerability Assessment, dowiadujemy się o bardzo dużej liczbie podatności naszych systemów IT. Często liczba wszystkich istniejących podatności sięga kilku tysięcy. Wśród nich znajdują się podatności, których wykorzystanie przez przestępców lub złośliwe programy może doprowadzić do poważnych konsekwencji dla firmy. W sytuacji gdy organizacja używa narzędzi Vulnerability Assessment, możliwe jest dokonanie ich integracji z SecureVisio. Raport ze skanera podatności (np. Rapid7 Nexpose) jest poddawany analizie przez SecureVisio, w celu wyselekcjonowania luk bezpieczeństwa najgroźniejszych dla działalności organizacji. Dzięki temu w praktyce możliwe staje się zarządzanie podatnościami w skali całej organizacji i unikanie incydentów w najważniejszych systemach IT. Firmy, które nie mają skanerów podatności, mogą poprzez SecureVisio zarządzać podatnościami z użyciem bazy Common Vulnerabilities and Exposures (CVE).
Narzędzia SecureVisio umożliwiają także symulację różnego rodzaju awarii sieci, zabezpieczeń i systemów IT. Dla przykładu, możemy zasymulować awarię serwera fizycznego. SecureVisio od razu poinformuje nas, które systemy IT będą niedostępne w wyniku tej awarii oraz które wspierane przez te systemy IT procesy biznesowe zostaną zakłócone i jakie będą wynikające z tego straty dla organizacji. Podobnie możemy symulować awarie urządzeń sieci i zabezpieczeń i dzięki temu oceniać, czy ryzyko biznesowe z tym związane jest akceptowalne dla organizacji.

IT GRC JAKO INTELIGENTNA PLATFORMA SOC

SecureVisio znajduje zastosowanie w każdej organizacji bez względu na wielkość i branżę. Może być używane jako samodzielne rozwiązanie IT GRC, wspomagające osoby odpowiedzialne za bezpieczeństwo firmy, lub zostać zintegrowane z systemami SIEM i wykorzystane jako inteligentna platforma do budowy Security Operations Center (SOC). Zbudowanie SOC bez narzędzi IT GRC wymaga stworzenia i utrzymywania wielu dokumentów opisujących powiązania obszarów biznesowych i informatyki. SOC to nie jest SIEM! SOC to scentralizowana jednostka, która zajmuje się kwestiami bezpieczeństwa na poziomie organizacyjnym (biznesowym) i technicznym. SIEM i inne narzędzia zarządzania bezpieczeństwem IT działają w obszarze technicznym – operują na adresach IP i numerach portów. Operatorzy SOC widzą sytuację w systemie informatycznym w kontekście procesów biznesowych firmy oraz bezpieczeństwa informacji i usług IT stanowiących największą wartość dla organizacji.

SecureVisio pomaga organizacjom w efektywnym kosztowo spełnieniu wymagań prawa i standardów bezpieczeństwa, jak wymagania KNF, GIODO, ISO-2700[1] i PCI-DSS. Elektroniczna dokumentacja SecureVisio wyposażona jest w kreator definiowania wymagań bezpieczeństwa. Wymagania mogą odnosić się do zabezpieczeń sieciowych, zabezpieczeń lokalnych oraz narzędzi zarządzania bezpieczeństwem. Na tej podstawie dokonywana jest automatyczna ocena zgodności istniejącego lub planowanego systemu zabezpieczeń z wymaganiami bezpieczeństwa. W trakcie użytkowania SecureVisio możliwe jest dostrajanie oraz definiowanie nowych wymagań bezpieczeństwa organizacji zgodnie z rzeczywistymi potrzebami.

[1] *Dla banków i innych instytucji finansowych w Polsce wymagania odnośnie do zapewnienia współpracy obszaru biznesowego, technologii informacyjnej i bezpieczeństwa przedstawiła Komisja Nadzoru Finansowego. Więcej informacji: http://www.knf.gov.pl/regulacje/praktyka/wytyczne_IT.html*



RYSUNEK 2. SECUREVISIO JAKO INTELIGENTNA PLATFORMA SOC

PODSUMOWANIE

Współczesna, realistyczna strategia bezpieczeństwa zakłada, że nie można uniknąć wszystkich incydentów bezpieczeństwa IT w organizacji. Należy przygotować się do szybkiego wykrywania incydentów w najważniejszych systemach IT, zanim dojdzie do naruszeń bezpieczeństwa. Rozwiązanie SecureVisio umożliwia organizacjom efektywne zarządzanie bezpieczeństwem IT, skoncentrowane na ochronie biznesu firmy, i dzięki temu swobodę rozwoju działalności biznesowej bez obawy o bezpieczeństwo.

SecureVisio i inne dobrej klasy rozwiązania IT GRC umożliwiają automatyczną ocenę biznesowego znaczenia zdarzeń w systemie zabezpieczeń technicznych (np. alarmów firewall i IPS, alarmów SIEM) i dzięki temu szybkie wykrywanie incydentów w systemach IT najważniejszych dla organizacji, zanim dojdzie do naruszeń bezpieczeństwa (tj. zablokowania ważnych procesów biznesowych, wycieku poufnych danych, utraty reputacji i zaufania klientów). Inteligencja i kontekst biznesowy, jakie SecureVisio wnosi do systemu zabezpieczeń technicznych sprawiają, że administratorzy zabezpieczeń koncentrują uwagę na systemach IT pełniących najważniejszą rolę w organizacji. Osoby odpowiedzialne za bezpieczeństwo podejmują poprawne decyzje, mając wiedzę i świadomość wartości chronionych systemów IT dla firmy, m.in. jak ważne są procesy biznesowe wspomagane przez systemy IT, czy w systemie IT znajdują się poufne dane wymagające szczególnej ochrony.

Zastosowanie SecureVisio w projektach IT zapewnia obniżenie kosztów bezpieczeństwa. Efektywny kosztowo rozwój bezpieczeństwa IT w organizacji możliwy jest m.in. dzięki funkcji automatycznego szacowania ryzyka biznesowego, której wyniki umożliwiają inwestowanie w zabezpieczenia IT tam, gdzie ma to największe uzasadnienie dla firmy.

Inna ważna korzyść SecureVisio to zmniejszenie stresu i ułatwienie pracy osób odpowiedzialnych za bezpieczeństwo. Dzięki funkcjom wspomagającym podejmowanie decyzji praca ludzi staje się łatwiejsza i mniej stresująca, m.in. w jednym miejscu dostępna jest automatycznie rozwijana elektroniczna dokumentacja zabezpieczeń IT, wspomaganie decyzji odbywa się za pomocą bazy wiedzy ekspertów bezpieczeństwa IT, automatycznie wykonywane jest szacowanie ryzyka, ocena wpływu incydentu i szacowanie wielkości strat dla organizacji.

O autorze:
Anna Grzesiakowska, doświadczony konsultant i audytor bezpieczeństwa w firmie eSECURE. Specjalizuje się w tematyce zapewnienia zgodności systemów informatycznych z wymaganiami prawa oraz zarządzania bezpieczeństwem organizacji w obszarze IT. Kontakt: anna.grzesiakowska@esecure.pl.

Anna Grzesiakowska, eSECURE