MAGAZYN

www.magazyn.mediarecovery.pl

INFORMATYKI ŚLEDCZEJ I BEZPIECZEŃSTWA IT

Security Operations Center jako koncepcja systemu bezpieczeństwa

WYWIAD Z PRZEMYSŁAWEM KREJZĄ

Czy możemy się ustrzec przed **zaawansowanym APT?**

GRZEGORZ MUCHA

Bezpieczna jakość

PRZEMYSŁAW SZCZUREK
MICHAŁ GLUSKA

Jak skutecznie **walczyć z malware**

TOMASZ PIETRZYK

SIEM czyli jak efektywnie zarządzać informacją i zdarzeniami bezpieczeństwa.

ADRIAN WRÓBEL

MAGAZYN
INFORMATYKI ŚLEDCZEJ I BEZPIECZEŃSTWA IT

Już teraz dostępny **online** na:

WWW.MAGAZYN.MEDIARECOVERY.PL

Od redakcji

Obecny numer, poświeciliśmy w całości podejściu określnym mianem Security Operations Center (SOC). Wynika to z kilku powodów. Obecnie nie wystarczy wdrożenie pojedynczego rozwiązania w zakresie bezpieczeństwa IT, ponieważ zagrożenia dotykają organizacje z wielu stron. Ponadto incydenty jeśli już zostaną wykryte to często nie jest możliwe wskazanie ich źródła i zabezpieczenia dowodów przestępstwa. Spowodowane jest to brakiem korelacji informacji pomiędzy różnymi rozwiązaniami z zakresu bezpieczeństwa. Jedynie holistyczne podejście jakie oferuje koncepcja Security Operations Center czyli połączenie bezpieczeństwa IT, informatyki śledczej, a także procedur oraz ludzi, sprawia że specjaliści otrzymują narzędzie, pozwalające im w czasie rzeczywistym reagować na zagrożenia, które do tej pory były niezauważalne oraz gromadzić i zabezpieczać dowody cyfrowe.

Wierzymy, że po lekturze najnowszego Magazynu, wielu z Państwa lepiej zrozumie czym jest SOC i jak może pomóc organizacji w podnoszeniu bezpieczeństwa IT na wyższy poziom. A dla tych którzy chcą zobaczyć na żywo Security Operations Center, zapraszamy do siedziby Mediarecovery.

Redakcja

Security Operations Center
jako koncepcja systemu bezpieczeństwa
Wywiad z Przemysławem Krejzą

Kradzież informacji, backdoor, haktywizm, APT, to wszystko wiele i zarazem nic nie znaczące slogany, które w ostatnim czasie przewijają się przez wszystkie tytuły gazet. Poczucie zagrożenia, które odczuwamy w odniesieniu do naszych cennych danych powoduje, że co rusz zastanawiamy się, czy aby na pewno jesteśmy dobrze zabezpieczeni.

Z Przemysławem Krejzą, Dyrektorem d/s Badań i Rozwoju Mediarecovery, CISSP i EnCE, ekspertem w zakresie informatyki śledczej i bezpieczeństwa IT rozmawia Damian Kowalczyk.

Dlaczego systemy bezpieczeństwa w organizacjach są zawodne?

Bezpieczeństwo informacji należy oceniać przez pryzmat ryzyka - nie sposób jest zabezpieczyć się przed każdym możliwym zagrożeniem, bo to kosztowałoby po prostu zbyt dużo. Każdy z nas odpowiedzialnych za bezpieczeństwo informatyczne w organizacjach, wie jak trudno jest zbudować uzasadnienie biznesowe dla czysto hipotetycznego zagrożenia. Oczywiście w większości zarządów firm istnieje świadomość, że przysłowiowe „włamania" są możliwe, jednak na pytanie: „ile mieliśmy takich problemów?" zwykle pada odpowiedź: „no, jeszcze nie mieliśmy (prawdopodobnie)". Nie bez znaczenia jest również wiara w szeroko pojęty antywirus. Nawet Brian Dye, wiceprezes Symantec – jednej z najbardziej znanych firm antywirusowych, powiedział niedawno, że czas posłać tego typu zabezpieczenia na emeryturę. Z drugiej strony wiemy, że najsłabszym ogniwem naszych systemów bezpieczeństwa są ludzie. Jeśli spojrzymy na statystyki lub przeczytamy key studies dużych incydentów, dowiemy się, że w większości przypadków zawiódł człowiek. Można by powiedzieć, że „w każdym z nas jest hacker" – poprzez swoje zaniedbania, podatność na socjotechnikę, czy zwykłą niewiedzę, niejako własnymi rękami otwieramy drzwi, którymi wchodzi ata-

kujący. Oczywiście możemy zwiększyć ilość systemów bezpieczeństwa i lepiej wyszkolić pracowników. Nie to jest jednak zasadniczą przyczyną zawodności systemów bezpieczeństwa. Prawdziwy problem tkwi głębiej – brak centralizacji zarządzania bezpieczeństwem nie daje właściwego poglądu sytuacyjnego na istniejące zagrożenia. Za całość bezpieczeństwa informacji zwykle odpowiada kilka zespołów, które często nawet nie wiedzą o swoich problemach. IT „widzi swoje", sieciowcy „swoje", ryzyko „swoje", itd. Brak jest jednego spojrzenia na nasze aktywa. To właśnie jest najsłabszy punkt systemów bezpieczeństwa.

SOC to koncepcja organizacji samouczącej się, w której poszczególne komponenty systemu bezpieczeństwa – antywirus, IDS/IPS, firewall, itd. – dostarczają informacji do centralnego systemu zarządzania.

Co możemy zrobić w takiej sytuacji?

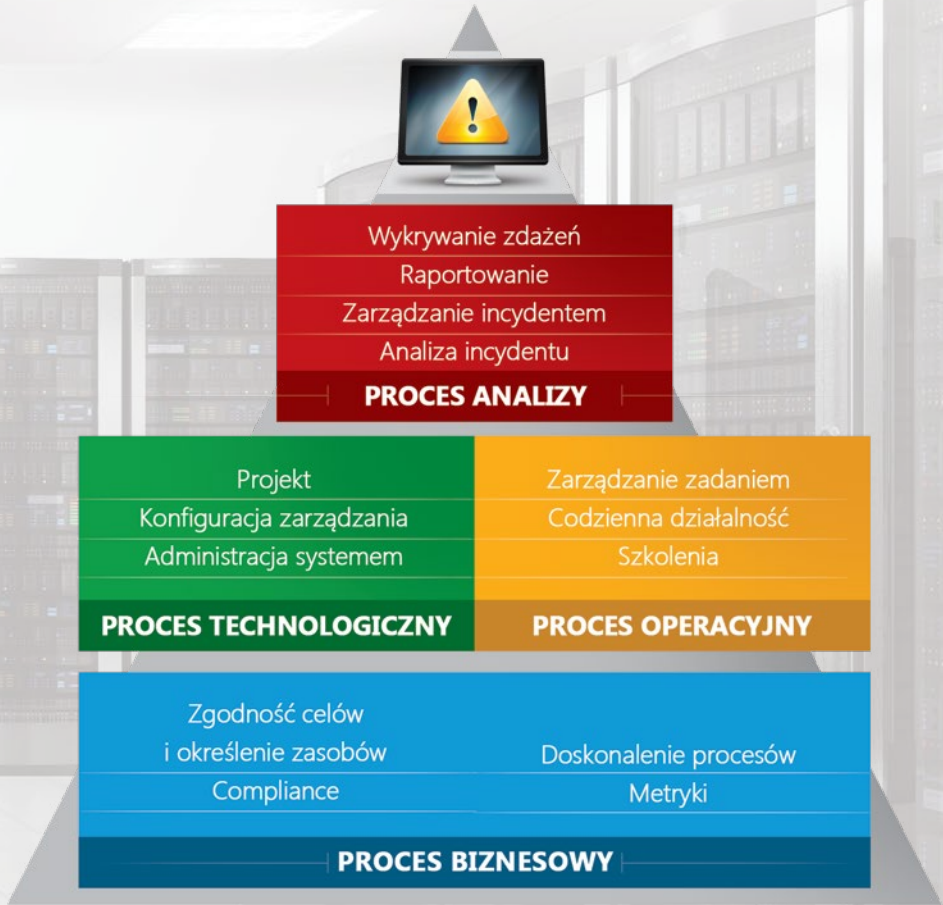
To co możemy zrobić to lepiej wykorzystywać to, czym dysponujemy poprzez zbudowanie świadomości sytuacyjnej stanu bezpieczeństwa w naszej organizacji. Koncepcja Security Operations Center, w uproszczeniu, sprowadza się do powiązania ze sobą różnych systemów w celu „zbudowania wiedzy". Agregowanie dostępnych informacji w jednym miejscu i ich korelacja pozwala odnaleźć szereg problemów związanych z bezpieczeństwem, które do tej pory były niezauważalne. Powiązanie ruchu sieciowego z tym co dzieje się na stacji roboczej może np. ujawnić szkodliwe oprogramowanie, które ukrywa się w naszym systemie.

Czy tego problemu nie rozwiązuje SIEM?

Nie mówimy tu o klasycznym SIEM. Wielu ekspertów mówiąc o SOC, w rzeczywistości ma na myśli właśnie tego typu system. SIEM jest oczywiście ważnym składnikiem SOC jednak tu potrzebne jest coś więcej. SOC to koncepcja organizacji samouczącej się w której poszczególne komponenty systemu bezpieczeństwa – antywirus, IDS/IPS, firewall, itd. – dostarczają informacji do centralnego systemu zarządzania. Aby to jednak miało sens, muszą w nim funkcjonować odpowiednie role organizacyjne w ramach spójnego zespołu. Zadaniem SOC jest dostarczenie dla każdej z ról pełnego ale, tylko niezbędnego poziomu informacji. Najważniejszy jest tu manager SOC, który ma pełną świadomość problemów na podstawie statusów systemów, stanu zarządzania incydentami i wiedzy o obciążeniach zespołów. Priorytet zarządzania zależny jest od wartości biznesowej, zasobów objętych konkretnymi zdarzeniami, a uporządkowany mechanizm komunikacji z IT czy z osobami odpowiedzialnymi za sieć informatyczną, pozwala menedżerowi na koordynowanie ich działań. SOC jest więc nie tylko rozwiązaniem technicznym, ale i organizacyjnym. Punkt ciężkości SOC odnosi się do decyzji w zakresie reakcji. Dostarczane do systemu dane muszą być na tyle precyzyjne aby zespół reagowania czy też informatyki śledczej mógł dotrzeć do źródła problemu. Tu zwykły SIEM, operujący głównie na metadanych, z reguły przestaje być wystarczający. Im więcej informacji jest dostępnych bezpośrednio, tym reakcja będzie skuteczniejsza. Zespół reagowania może potrzebować dostępu do wszystkich warstw ruchu sieciowego, pamięci stacji roboczych, itd. Oczywiście wszystko zgodnie z zasadami informatyki śledczej – a więc, z możliwością przedstawienia dowodów w sądzie.

Brzmi to na skomplikowany i kosztowny proces...

Decyzja o centralizacji bezpieczeństwa w centrum operacyjnym nie jest łatwa. Model, o którym powiedziałem wcześniej, wymaga pewnych zmian organizacyjnych, a przede wszystkim ewolucji modelu myślenia. Jednak odpowiednie zaplanowanie tego procesu pozwala na przeprowadzanie zmiany stopniowo, z wykorzystaniem dostępnego zespołu



HIERARCHIA PROCESÓW W RAMACH SOC

i istniejących komponentów systemu bezpieczeństwa. Również decyzje zakupowe mogą być odłożone w czasie, a co więcej bardziej świadome bo oparte o zgromadzoną w SOC wiedzę o incydentach.

Od czego powinniśmy zacząć?

Pierwszym krokiem do podjęcia decyzji czy SOC powinien zadziałać w organizacji jest oczywiście ocena wartości biznesowej przetwarzanych informacji, istniejących wymogów prawa, itd. Podzielam zdanie Nicka Bradleya z IBM, który zaleca rozważanie najgorszych hipotetycznych scenariuszy. Jeśli skutki możliwych naruszeń bezpieczeństwa mogą wywołać poważny kryzys – SOC będzie nieunikniony w przyszłości. Kolejny krok to powołanie managera SOC w osobie dyrektora ds. bezpieczeństwa informacji (CIO), w celu ustalenia w nim odpowiedzialności wykonawczej. Pierwszą inicjatywą powinien być przegląd dostępnych systemów i możliwości pozyskiwania z nich wiedzy. Celem tych działań powinno być zbudowanie świadomości sytuacyjnej. Fundamentem programu SOC jest uporządkowanie pełnego wykazu aktywów informacyjnych. Wiele firm nie przywiązuje do tego wielkiej wagi, traktując system IT jako jedność. A przecież wiemy, że niektóre serwery czy stacje robocze posiadają cenniejsze informacje. Inwentaryzacja aktywów jest trudna choć wymaga tego chociażby norma ISO 27001. Techniczne funkcjonowanie SOC powinno być oparte o SIEM. Dobre rozwiązanie tego typu powinno zapewnić w przyszłości możliwość podziału ról zespołów, zgodnie z tym o czym mówiłem wcześniej. Szczególny nacisk przy wyborze rozwiązania powinien być położony na możliwość szybkiego dotarcia do źródła problemu na wypadek incydentu.
Funkcjonalność SOC powinna dążyć do maksymalizacji ilości informacji na temat bezpieczeństwa - ich gromadzenia i przechowywania, nawet jeśli nie ma możliwości bieżącej analizy.

Często retencja danych w komponentach systemu bezpieczeństwa nie przekracza tygodnia lub dwóch. To powoduje, że jeśli firma wykryje naruszenie, nie ma możliwości zbadania problemu. Nawet dane z pozoru zbędne mogą okazać się przydatne w trakcie analizy incydentu. Ważne również, aby dane te były dostępne szybko. Te aspekty powinny być brane pod uwagę przy wyborze rozwiązań.

Czy utrzymanie SOC jest kosztowne?

Tak jak mówiłem SOC jest raczej ewolucją niż rewolucją i może wymagać jedynie reorganizacji. Może się jednak zdarzyć, że budowanie świadomości sytuacyjnej bezpieczeństwa doprowadzi do wniosku, że któryś z obszarów nie jest pokryty. Niewiedza ta może prowadzić do przeoczenia pewnych zagrożeń. Konieczne może być wówczas zaplanowanie dodatkowych komponentów systemu bezpieczeństwa. Kluczem do decyzji powinno być lepsze monitorowanie, ale w odniesieniu do tego jakie dane i systemy muszą być chronione a nie jakie są możliwość danego produktu. Możliwe jest również rozważenie czy nie powierzyć części zadań na zewnątrz. Decyzje w tym zakresie są zależne są od zakładanych negatywnych scenariuszy. Niektóre role zespołów, np. informatyka śledcza może być skutecznie realizowana w ramach umów outsourcingowych.

Jakie jeszcze mamy korzyści z SOC?

Dobry system bezpieczeństwa zorientowany jest na samodoskonalenie. Oznacza to, że każda sytuacja kryzysowa powinna pozwolić na bycie lepszym w przyszłości. Security Operations Center poprzez zorientowanie na wyjaśnianie incydentów pozwala na unikanie kryzysów i wyciąganie wniosków z występujących problemów. Świadomość sytuacyjna dostarczana poprzez wiedzę z istniejących systemów bezpieczeństwa pozwala łatwo określić stan normalności, a każde odchylenie od tego stanu, wywołane nawet przez całkowicie nieznane zagrożenie będzie w SOC zauważalne. Uporządkowane role zespołów powodują, że w takiej sytuacji każdy będzie wiedział co robić. Z drugiej strony SOC dostarczy nam wiedzy niezbędnej do zarządzania ryzykiem. Pozwala na tworzenie lepszych uzasadnień dla biznesu i świadome budowanie systemu bezpieczeństwa, poprzez wdrażanie nowych komponentów w ramach SOC.

Czy możemy się ustrzec przed zaawansowanym APT?

Grzegorz Mucha

W miarę rozwoju technik ataków i środków na nie przeznaczanych, a niejednokrotnie również wsparcia służb wrogich państw, musimy się zacząć przyzwyczajać do myśli, że nasza z trudem budowana ochrona nie gwarantuje pełnego bezpieczeństwa. Co więcej, głównym mottem współczesnych przestępców jest „powoli, cierpliwie, po cichu". W większości przypadków możemy się spodziewać, że wroga obecność zostanie odkryta po tygodniach czy nawet miesiącach od wejścia do systemu IT. Dlaczego?

Środowiska informatyczne stają się coraz bardziej złożone i coraz trudniejsze do spójnego monitorowania, a zarządzaniem nimi zajmuje się coraz większa liczba osób. Występujące nierzadko wewnętrzne animozje pomiędzy tymi grupami (związane np. z konkurowaniem o ten sam budżet) nie ułatwiają komunikacji i tworzą precedensy utrudniania czy opóźniania dostępu do informacji. Kolejny powód to coraz większe wymagania samych użytkowników – mobilność, dostęp z każdego miejsca i każdego urządzenia, a równocześnie minimum utrudnień. Nie można też zapomnieć o współpracujących z nami firmach czy konsultantach zewnętrznych, wobec których, co do zasady, kontrola jest ograniczona. Często okazuje się, że choć obca obecność zostaje w końcu wykryta, problemem jest czas, jaki upłynął od ataku do wykrycia, zrozumienie w jaki sposób przestępca przeniknął systemy obrony (i jak może to zrobić ponownie), określenie jakie szkody spowodował, i wreszcie brak jest możliwości szybkiej oraz skutecznej reakcji. Celem takiej reakcji powinno być nie tylko powstrzymanie wykrytej obecności, ale minimalizacja strat biznesowych, reewaluacja ryzyka i wdrożenie odpowiednich działań naprawczych.

W wielu organizacjach alokacja środków skupiona jest na obszarze prewencji co wpływa na zmniejszenie budżetów operacyjnych przeznaczonych na bezpieczeństwo. W efekcie rośnie ilość systemów do zarządzania, zaś obsługą zdarzeń bezpieczeństwa zajmują się administratorzy, których podstawowym zadaniem jest utrzymanie tychże systemów. Najwyższy czas uznać, że głównym celem działań w zakresie bezpieczeństwa jest ochrona wartości biznesowych organizacji, a nie zapobieganie włamaniu samemu w sobie. Najlepszym sposobem zapobiegania stratom biznesowym jest szybka identyfikacja oraz reakcja na atak. Aby to osiągnąć organizacje powinny przenieść część środków na inwestycję w inteligentne systemy rozszerzające możliwości wykrywania i odpowiedzi na skomplikowane ataki. Systemy takie muszą umożliwić pełny wgląd w środowisko IT oraz wykorzystywać zewnętrzne źródła informacji o zagrożeniach.

SOC i Intelligence-driven Security

Grupa Security for Business Innovation Council, zrzeszająca osoby zarządzające bezpieczeństwem w największych firmach, zaproponowała nowe podejście do ochrony krytycznych informacji i zasobów biznesowych, nazwane „intelligence-driven security". Główną tezą jest ograniczenie polegania na systemach statycznej ochrony i rozwiązaniach bazujących na sygnaturach, potrafią identyfikować typy ataków, które wydarzyły się już w przeszłości. Zamiast tego należy

poszukiwać podejrzanych aktywności i wzorców nietypowych w konkretnym środowisku. Narzędziem do wdrożenia tego zalecenia jest utworzenie dedykowanego centrum ds. bezpieczeństwa, czyli SOC-u (SOC – Security Operations Center).

Aby SOC był skuteczny, musi być zbudowany niezależnie od istniejącego centrum zarządzania infrastrukturą. Zadaniem SOC nie jest bowiem codzienne utrzymanie środowiska i reagowanie na awarie. Centrum ds. bezpieczeństwa ma skupiać się wyłącznie na incydentach bezpieczeństwa i ich jak najszybszym rozwiązywaniu. Ponadto SOC, musi widzieć całą organizację jako jeden organizm, a jego szef najlepiej, żeby podlegał bezpośrednio pod zarząd, a sam system musi łączyć w sobie technologie, odpowiednie procesy oraz dedykowany personel.

Z tej trójki najmniej myśli się o procesach – a SOC powinien być odpowiedzialny za regularną ocenę ryzyka ataku, szacowanie wektorów ataku, badanie zagrożeń, szacowanie stanu bezpieczeństwa i ciągłe podnoszenie stopnia dojrzałości organizacji przez projektowanie i testowanie planów zarządzania odpowiedzią na atak – zarówno ze strony technologicznej, jak i organizacyjnej (np. wyznaczone procedury współpracy w działem prawnym oraz działem PR). Osoby pracujące w SOC nie mogą się równocześnie zajmować administrowaniem systemami lub innymi zadaniami w dziale IT. Ich zadaniem jest rozpoznanie incydentu, jego ocena oraz przedsięwzięcie adekwatnych działań w jak najkrótszym czasie. SOC musi zatrudniać osoby lub współpracować z zewnętrznymi ekspertami w dziedzinie informatyki śledczej, analityki danych, analizy zagrożeń. Kwalifikacje takich osób powinny być regularnie podnoszone, i jest to zadanie managera SOC. Pracownicy SOC obsługujący incydenty powinny mieć odpowiednie prerogatywy nadane przez zarząd, aby nie okazało się, że śledztwo w sprawie krytycznego incydentu nagle staje na kilkanaście godzin, ponieważ jest weekend i śledczy musi oczekiwać na uzyskanie zgody na dostęp do jakiegoś systemu w celu zebrania dowodów do poniedziałku, kiedy w pracy będzie odpowiedni manager – a istnieje ryzyko, że w tym czasie dowody zostaną zniszczone lub utracone.

Zadaniem SOC nie jest bowiem codzienne utrzymanie środowiska i reagowanie na awarie, SOC ma skupiać się na incydentach bezpieczeństwa i ich jak najszybszym rozwiązywaniu.

Zostały jeszcze technologie – tu można by wyróżnić kilka kluczowych wymagań:

- skalowalna analityka, czyli mechanizmy umożliwiające analizę dużych ilości ciągle zmieniających się danych w czasie bliskim rzeczywistemu
- hurtownia danych, zbierająca wszelkie informacje związane z bezpieczeństwem w jednym miejscu, powiązane wzajemnie między sobą i dostępne dla mechanizmów analitycznych
- elastyczna architektura systemów monitorowania, umożliwiająca zbieranie danych z różnych źródeł i w różnych formatach, ich indeksowanie, normalizację i analizę
- centralna konsola do prowadzenia śledztw i do zarządzania odpowiedzią na incydent
- nagrywanie ruchu sieciowego, dające możliwość rekonstrukcji sesji sieciowych, czy wyciągnięcie przesłanych plików do analizy
- integracja z wewnętrznymi źródłami danych np. o zasobach wewnętrznych, ich znaczeniu biznesowym dla organizacji
- integracja z zewnętrzną informacją o zagrożeniach, możliwość korelacji tych danych z pozyskanymi informacjami o zdarzeniach i ruchu sieciowym

SOC musi zatrudniać osoby lub współpracować z zewnętrznymi ekspertami w dziedzinie informatyki śledczej, analityki danych, analizy zagrożeń.

Jak to można robić - przykład

Dobrym przykładem na realizację idei SOC-a jest CIRC (Critical Incident Response Center) firmy EMC, który zbiera informacje z całej organizacji i stanowi centralny punkt monitorowania oraz wymuszania bezpieczeństwo i integralności zasobów firmy. CIRC zbiera dane m.in. z ponad 1,400 urządzeń zabezpieczających i 250,000 komputerów rozsianych w 500 lokalizacjach na całym świecie.

W ramach CIRC zespół specjalistów monitoruje globalne środowisko IT EMC, odpowiada na zagrożenia i podatności - od malware'u i wycieku danych po czysto fizyczne jak kradzież sprzętu. CIRC prezentuje działania swojej pracy bezpośrednio do wyższego managementu, co pozwala na skuteczne wdrożenie idei ciągłej poprawy stanu bezpieczeństwa organizacji.

W CIRC wykorzystywane są różne narzędzia, jednak serce systemu stanowią rozwiązania RSA Archer i RSA Security Analytics. Te dwa systemy integrują dane pochodzące z innych narzędzi i dają perso-

nelowi CIRC jedno spójne repozytorium informacji i centralny punkt zarządzania. Integracja rozwiązań pozwala na zbudowanie skutecznego przepływu danych i sterowania pracą, a co za tym idzie wpływa na przyspieszenie obsługi incydentów i zmniejszenie czasu ich zamknięcia.

Codziennie do CIRC trafiają setki alarmów. Zanim alarm zostanie przesłany analitykowi do dalszego śledztwa, jest automatycznie korelowany z zestawem danych związanych z incydentem. W celu integracji danych kontekstowych i zewnętrznych informacji w procesie wykrywania oraz odpowiedzi na incydent zostało specjalnie opracowanych kilka procesów i technologii. Jedną z nich jest m.in. system wskazywania na zagrożenie w oparciu o informacje z wewnętrznych i zewnętrznych źródeł, informacji od partnerów i własnego zespołu FirstWatch. Wskaźniki zagrożeń (IOC – Indicators of Compromise) obejmują szeroki zakres informacji, od podejrzanych adresów IP i wrogich domen, do charakterystyk komunikacji, takich jak specyficzne nagłówki maili. Wskaźniki są klasyfikowane względem poziomu ważności (severity) i automatycznie przekazywane do Security Analytics jako tzw. feed, który pozwala na wygenerowanie dodatkowych metadanych. Na przykład znana z ataków APT domena wygeneruje metadaną o wartości „Severity 1" dla każdej aktywności, w której pojawi się ta domena. Alarmy oparte o nią są przesyłane do konsoli Archera, gdzie mogą utworzyć lub uzupełnić incydent. Zanim jednak alarm dotrze do analityka, z centralnej bazy CIRC dołączane są do opisu sesji dodatkowe elementy, pomagające analitykowi zobaczyć pełen kontekst zdarzenia.

Automatyczna analiza końcówek

Wspomnieliśmy o logach i analizie ruchu sieciowego, ale nie sposób pominąć serwery i stacje końcowe użytkowników. Systemy antywirusowe oraz hostowe IPS-y, które wciąż bazują głównie na sygnaturach, coraz trudniej wykrywają współczesny malware i są zupełnie nieskuteczne wobec ataków celowanych typu APT. Z tego powodu EMC CIRC wdrożyło rozwiązanie ECAT (Enterprise Compromise Assessment Tool) jako dodatkowe narzędzie analizy, wykorzystywane do sprawdzania końcówek, co do których istnieje podejrzenie zarażenia lub innego rodzaju wrogiej obecności – na co może wskazywać np. analiza ruchu sieciowego z takiego komputera.

Żeby działania zespołu SOC były skuteczne, za jego stworzeniem musi iść wsparcie na poziomie zarządu firmy, oraz dobrze zdefiniowane i opisane procesy.

Rozwiązanie wykorzystuje wiele technik analizy komputera i wykrywa anomalie typowe dla zarażeń złośliwym oprogramowaniem, takich jak hooking, modyfikacje jądra systemu, modyfikacje uruchomionych procesów w pamięci, zmiany w rejestrach, ukrywanie komunikacji, itp. ECAT pozwala również błyskawicznie porównać stan systemu z czystym systemem wzorcowym i wykryć wszelkie odstępstwa. Analizę może przyspieszyć identyfikacja „dobrego" oprogramowania dzięki wykorzystaniu list znanych programów np. od Bit9. Na koniec analizy ECAT produkuje wynik (MSL – Machine Suspect Level), który wskazuje na prawdopodobieństwo, że stacja została skutecznie zaatakowana lub zarażona. Co więcej, dzięki zbieraniu wyników skanów do wspólnej bazy, analityk który zidentyfikuje podejrzany proces na komputerze może natychmiast sprawdzić, na jakich innych komputerach ten proces był uruchomiony. Analiza jest wykonywana na bardzo niskim poziomie, a zastosowane techniki praktycznie uniemożliwiają malware'owi ukrycie się przez ECAT-em. Zamiast polegać na pojedynczych technologiach organizacje powinny realokować część budżetu na stworzenie SOC-a opartego na takich rozwiązaniach, które umożliwią szybką i pełną analizę zdarzeń, z wykorzystaniem co najmniej informacji z logów, pełnego ruchu sieciowego oraz stacji użytkowników, a także informacji wewnętrznych i zewnętrznych wzbogacających kontekst zdarzeń i dających odniesienie do wartości biznesowej chronionych zasobów. Technologie nie mogą żyć w oderwaniu od ludzi – SOC powinien być obsługiwany przez zespół stale podnoszących swoje kwalifikacje fachowców, którzy nie mają w swoich obowiązkach zajmowania się codziennym utrzymaniem systemów.

Ponadto żeby działania zespołu SOC były skuteczne, za jego stworzeniem musi iść wsparcie na poziomie zarządu firmy, oraz dobrze zdefiniowane i opisane procesy. Nie chodzi o wielkość organizacji, tylko o zasadę. Dokładnie te same potrzeby mają nasze rodzime firmy, dokładnie te same idee i te same technologie mają zastosowanie dla lokalnych SOC-ów.

Nikt nie mówi, że nie należy monitorować mniejszej infrastruktury, ani że SOC nie może na początek zatrudniać kilka osób. W końcu od ilości dużo ważniejsza jest skuteczność tych osób, a to można osiągnąć dzięki zaleceniom opisanym powyżej.

Autor jest Senior Systems Engineerem w RSA, the Security Division of EMC.

Jak skutecznie walczyć z malware

Tomasz Pietrzyk

Biorąc pod uwagę ciągle rosnącą liczbę zaawansowanych zagrożeń z jakimi firmy muszą się mierzyć każdego dnia, a szczególnie jeśli uwzględnimy ich zaawansowany poziom techniczny i nastawienie na uzyskanie określonych – głównie finansowych – celów, konieczna jest zmiana podejścia firm do obsługi incydentów bezpieczeństwa. Obraz zagrożeń wskazuje, że praktycznie nie ma aktualnie żadnego działu gospodarki lub firmy, które nie byłyby zagrożone przez zaawansowane ataki, przechodzące w niezauważony sposób przez najczęściej stosowane klasyczne zabezpieczenia (IPS, firewall, gateway'e).

Zaawansowane ataki mogą wiązać się ze zdalną kontrolą nad stacjami w sieci, a trudno sobie wyobrazić większe ryzyko niż sytuacja, w której nieautoryzowana osoba z zewnątrz może potencjalnie wykonywać w naszej sieci dowolne działania, a my nie jesteśmy ich świadomi i nie możemy ich kontrolować. Zagrożenie posiadania zdalnej kontroli nad naszymi zasobami tym bardziej powinno utwierdzać nas w przekonaniu, że sam fakt wykrycia ataku nie jest wystarczający do zamknięcia obsługi „zdarzenia". W praktyce to właśnie czynności podjęte po stwierdzeniu włamania decydują o tym jak dobrze organizacja jest przygotowana na atak i jak dobrze potrafi zminimalizować jego wpływ.

Nie ma aktualnie żadnego działu gospodarki lub firmy, które nie byłyby zagrożone przez zaawansowane ataki.

W przypadku obsługi incydentu bezpieczeństwa (ataku) możemy wskazać podstawowe fazy wymagane do właściwego postępowania w takiej sytuacji:

1. Wykrycie ataku (ang. detection) – bezpośrednie (np. alert z naszych systemów ochrony) lub pośrednie w postaci powiadomienia ze źródeł zewnętrznych (np. z CERT) o wykryciu połączenia z naszej sieci do serwerów powiązanych z atakami.

2. Zminimalizowanie skutków ataku (ang. incident response) – w idealnym przypadku „minimalizacja" oznacza niedopuszczenie do skutecznego wykonania ataku (zablokowanie ataku). Co najmniej oznacza to izolowanie zainfekowanych komputerów i nie pozwalanie na dalsze rozprzestrzenianie się ataku i niekontrolowanej działalności cyberprzestępcy w naszej sieci.

3. Analiza ataku (ang. forensic) – próba odpowiedzenia na pytania jak przebiegał atak (jakie narzędzia i wektory ataku były użyte), jakie były jego cele i skutki, skąd był prowadzony. Na tym etapie są też zwykle gromadzone dowody, które mogą pomóc w przeprowadzeniu formalnego postępowania przeciwko cyberprzestępcy. Jest to zwykle najbardziej czasochłonny i kosztowny etap obsługi incydentu.

4. Usprawnienie procedur i zabezpieczeń (ang. improvement) – wnioski z analizy ataku powinny być zgromadzone i przeniesione na zmiany w obowiązujących procedurach, konfi-

guracji i budowie systemów bezpieczeństwa celem lepszego przygotowania się do podobnych zdarzeń w przyszłości.
Cały proces jest realizowany i nadzorowany przez dział IT, a w coraz większej ilości organizacji przez wyspecjalizowaną komórkę, czyli SOC (Security Operation Center). Tutaj trafiają informacje z systemów bezpieczeństwa i stąd są inicjowane kolejne kroki obsługi incydentu. Sam SOC jest to więc zbiór narzędzi, specjalistów ds. bezpieczeństwa, procedur, ale i wiedzy o atakach, które opisują postępowanie w razie wystąpienia incydentu bezpieczeństwa. Wykrycie ataku to dopiero początek cyklu jego obsługi. Zaawansowane technicznie zagrożenia, nastawione na ukryte działanie, z jakimi współcześnie mają do czynienia organizacje, wymagają stosowania odpowiednich metod przeciwdziałania. Organizacje muszą być przygotowane na obsługę incydentów bezpieczeństwa o różnej skali, ryzyku i poziomie zagrożenia wnoszonym do prowadzonej działalności. Praktycznie nie ma aktualnie firmy, która nie byłaby narażona na zaawansowane ataki. Przygotowanie do odparcia ataku nie może ograniczać się tylko do wdrożenia najnowocześniejszych systemów wykrywania. Równie ważne są możliwości ograniczenia wpływu ataku, a także analiza przebiegu ataku dla zrozumienia jego skali, celów, zastosowanych technik i narzędzi. Właściwa obsługa procesu reakcji na atak wiąże się z oddelegowaniem tej obsługi do wyspecjalizowanych zespołów IT – w szczególności SOC. Integrowanie produktów między sobą, ale także ułatwienia w łączeniu ich z produktami innych producentów ma szczególne znaczenie w budowie centrów SOC, które z założenia muszą bazować na rozwiązaniach różnych dostawców. Jedną z firm, która konsekwentnie rozwija swoje rozwiązania pod kątem zapewnienia wsparcia dla Klientów na każdym etapie obsługi incydentów bezpieczeństwa jest FireEye. Innowacyjne, bezsygnaturowe systemy wykrywania zaawansowanych ataków w sieci i korelowania danych między różnymi wektorami ataku, rozwiązania detekcji ataków na bazie logów z różnych systemów IT, są uzupełnione rozwiązaniami działającymi na komputerach oraz pomiędzy systemami do analizy przebiegu ataku. Uzupełnieniem oferty wielu dostawców, w tym również FireEye są usługi, które Klienci wykorzystują w procesie budowy SOC, w obsłudze szczególnie ważnych i skomplikowanych incydentów bezpieczeństwa (usługi incydent response, forensic) jak również szkoleń dla specjalistów zajmujących się obsługą incydentów bezpieczeństwa.

Autor jest inżynierem systemowym w firmie FireEye. Od ponad 10 lat rozwija swoje doświadczenie i pasje, które są związane z dziedzinami bezpieczeństwa IT.

SIEM czyli jak efektywnie zarządzać informacją i zdarzeniami bezpieczeństwa

Adrian Wróbel

Budując SOC czyli Security Operation Center, tworzymy miejsce, w którym bezpieczeństwo IT, informatyka śledcza, a także procedury i ludzie współgrają ze sobą. Wymieniają się danymi pozyskiwanymi z wielu źródeł. Budują przejrzystość organizacji pozwalając zidentyfikować najbardziej podatne miejsca i zabezpieczyć je. SOC to miejsce, w którym dzięki synergii wielu rozwiązań oraz wymianie informacji pomiędzy nimi można osiągnąć to o czym mówimy od dawna czyli wyższy poziom bezpieczeństwa. Jednym z elementów SOC jest konieczność monitorowania i dostarczania informacji z wielu urządzeń. Infrastruktura IT w dzisiejszych organizacjach jest mocno skomplikowana. Stosujemy wiele urządzeń sieciowych nierzadko pochodzących od różnych producentów, serwery, macierze, komputery PC oraz laptopy, tablety czy też urządzenia mobilne takie jak smartfony. Każde z nich generuje tysiące przydatnych informacji, których analiza bez specjalistycznych narzędzi jest praktycznie niemożliwa. Bez wiedzy o stanie tych właśnie urządzeń nie ma mowy o żadnym poziomie bezpieczeństwa. SIEM czyli Security Information and Event Management będzie jednym z kluczowych rozwiązań pod kątem pozyskiwania informacji i monitorowania urządzeń. Przyjrzyjmy się bliżej temu rozwiązaniu i możliwością jakie daje.

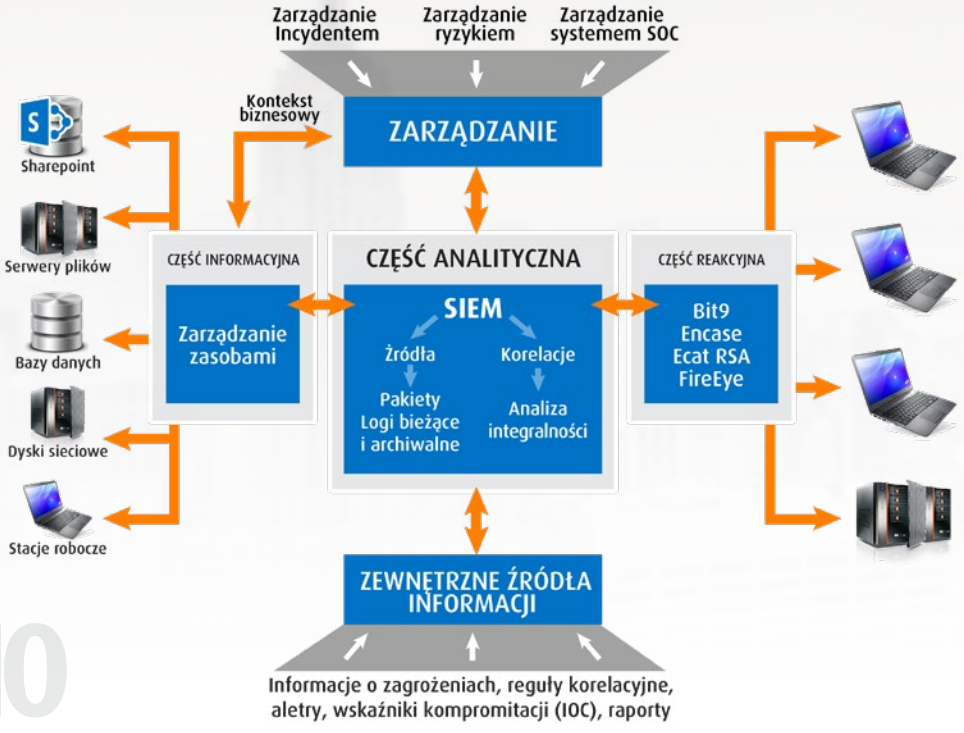
Warstwa technologiczna rozwiązań klasy SIEM pozwala na centralne zarządzanie logami generowanymi z wielu urządzeń w jednym czasie oraz ich archiwizację. W tym celu wszystkie informacje generowane przez urządzenia są przesyłane, gromadzone i scentralizowane. Ponadto silnik SIEM przechowuje informacje i udostępnia je Zespołowi Bezpieczeństwa w celu analizy, mapowania oraz generowania raportów i zarządzania w sytuacjach kryzysowych, zgodnie z określonymi procedurami. Możliwość korelacji czyli szukania zależności pomiędzy nimi daje działom bezpieczeństwa a także pracownikom SOC niespotykany dotąd poziom wiedzy. Korelacja danych jest podstawowym składnikiem monitoringu i analizy zebranych danych prowadzonych przez analityków pracujących w Security Operations Center (SOC). Działalność ta nie jest ograniczona jedynie do działań związanych z wcześniejszymi powiadomieniami alarmowymi, odpowiedziami w czasie rzeczywistym czy przygotowywaniem raportów. Obejmuje również wdrażanie zasad, procedur i rozwiązań, identyfikację, ocenę oraz sugestię środków uznanych za konieczne i pilne. To jest wartość dodana działalności, gdy jest prowadzone przez wysoko wykwalifikowanych analityków, którzy są odpowiedzialni za przygotowania i zarządzania

złożonymi projektami bezpieczeństwa. Z punktu widzenia zespołu odpowiedzialnego za bezpieczeństwo, SIEM jest jednym z podstawowych narzędzi do monitorowania. Umożliwia nie tylko szybkie pozyskanie informacji, ale również ich analizę, co przy odpowiednim doborze procedur i ludzi daje potężne narzędzie do zwalczana zagrożeń w sieci wewnętrznej. Technologicznie SIEM jest platformą do zarządzania informacjami oraz zdarzeniami. Jako platforma nie może jednak istnieć samodzielnie. Zaczynając od podstaw czyli zbierania danych z urządzeń i innych systemów bezpieczeństwa, SIEM po prostu nie może bez nich istnieć. Innymi słowy musimy mieć z czego zbierać informacje. Bez posiadanych podstawowych narzędzi jak kontrole dostępu, firewalle, antywirusy, antyspam, a także skorelowanie ich z urządzeniami sieciowymi albo komputerami i urządzeniami mobilnymi może okazać się, że SIEM jest „ślepy". Ponadto, SIEM sam w sobie, nie chroni nas przed zagrożeniami typu malware. Myślę, że o konieczności posiadania tego typu narzędzi nie trzeba nikogo przekonywać. Dzisiejszy rynek bogaty jest w szereg narzędzi do zabezpieczenia przed tego typu zagrożeniami jak FireEye czy Bit9 (whitelisting) pozwalających na uruchomienie tylko aplikacji i procesów znanych i zdefiniowanych. Idąc dalej SIEM nie ochroni nas przed wyciekiem – celowym lub przypadkowym – danych z naszej firmy. Aby lepiej zobrazować jak działa SIEM samodzielnie oraz w ramach Security Operation Center, posłużę się przykładem. Wyobraźmy sobie, że kilka komputerów w naszej sieci otrzymało zapytanie kierowane z nieznanego adresu IP. Następnie, na każdym z nich próbowano zalogować się na konto domeny AD (Active Directory) oraz poczty web. Co więcej, na skrzynki pocztowe pracowników przyszedł mail informujący o konieczności zalogowania się w usłudze pocztowej za pomocą zamieszczonego w wiadomości linku. Wiele z naszych komputerów połączyło się w tym czasie z zewnętrznym adresem. Została nawiązana komunikacja z serwisem, za pośrednictwem którego zainstalowano na tych komputerach oprogramowanie. Po kilku godzinach lub dniach od tego zdarzenia zainstalowane oprogramowanie znów połączyło się z zewnętrznym serwisem pobierając pliki. Po kilku kolejnych dniach komunikacja została wznowiona i od tamtego czasu w nieregularnych odstępach czasu wysyłane są spakowane i szyfrowane emaile (z reguły kilkadziesiąt kilobajtów danych) na zewnętrzny serwer. W przeciągu tych kilku dni wiele osób próbowało logować się do systemów, do których nie mają i nie potrzebują dostępu. Co więcej robili to podszywając się pod inne osoby. Jest to opis jednego z ataków APT (Advanced Persistent Threats). Czytając powyższy przykład zapewne wiele osób zastanawia jak tak trywialny atak może się udać? Otóż nie tylko może, ale bardzo często kończy się sukcesem. Zebranie danych z tak wielu źródeł, a co więcej połączenie ich między sobą bez odpowiednich narzędzi jak SIEM jest niewykonalne. Bo to właśnie SIEM poprzez korelację logów prześle alerty dotyczące nieudanych prób logowania oraz masowego wysyłania pakietów danych. Co więcej zbierze dane z innych źródeł, które mogą generować swoje alerty jak np. firewall, system antyspamowy czy black listy dotyczące serwisów WWW. Sam SIEM pozwoli nam nie tylko na szybkie wykrycie takiego incydentu, ale również odpowiednie zareagowanie na niego. W przypadku Security Operation Centers taki atak praktycznie skazany jest na porażkę. SIEM współpracując z innymi technologiami pozwoli mu zapobiec.

Za pośrednictwem rozwiązania do analizy APT (malware) umożliwi analizę pobranego pliku i wykrycie malware'u. Wspólnie z rozwiązaniem do zarządzania tożsamością oraz kontrolą dostępu do systemów informatycznych nie pozwoli na zmianę uprawnień czy też zasygnalizuje próbę zalogowania się przez uprzywilejowanego użytkownika, na urządzeniu, z którego nigdy tego nie robił. Poprzez mechanizmy monitorowania sesji będziemy mogli wychwycić podejrzane akcje na serwerach i bazach, a następnie zapobiec kopiowaniu poufnych danych. Wreszcie rozwiązania do whitelistingu odpowiednio zabezpieczą nasze komputery przed instalacją i uruchomieniem nieznanego oprogramowania. Na zakończenie narzędzia do analizy incydentów i pozyskiwania danych cyfrowych dokonają przeszukania ogromnych ilości danych i zabezpieczą zebrany materiał do dalszego wykorzystania np. jako materiał dowodowy w sądzie. Podsumowując Security Operations Center nie może składać się jedynie z systemu SIEM, ponieważ tylko ścisła współpraca kilku narzędzi może stworzyć kompletną platformę do zarządzania bezpieczeństwem. Z drugiej strony SIEM funkcjonujący osobno nie jest tak efektywny jak wtedy kiedy stanowi element SOCa. Ponadto w całym procesie niezbędni są również ludzie oraz procedury.

Autor jest konsultantem w laboratorium Mediarecovery.

Przykładowa architektura systemu SOC



Bezpieczna jakość

Michał Gluska, Przemysław Szczurek

We współczesnym otoczeniu gospodarczym firmy i organizacje dążą do stabilizacji, której wymiernym celem jest osiąganie trwałych sukcesów operacyjno – biznesowych. Jego osiągnięcie jest możliwe poprzez skuteczne zarządzanie organizacją – zarówno w ujęciu relacji z klientem, jak i ochrony własnych interesów, które stanowią podstawę dla budowania efektywnego zorientowania na rynek i odbiorcę. Słuszną wydaje się więc kompilacja dwóch popularnych, ale przede wszystkim wiarygodnych narzędzi zarządzania, którymi są mechanizmy norm **ISO 9001 i ISO 27001**. Przed prawie 30 laty na rynkach ogólnoświatowych pojawiło się narzędzie, jakim jest norma ISO 9001. Wydawało się, że oto znaleziono sposób na uporządkowanie zagadnienia, jakim jest zapewnienie jakości. Norma ta bowiem zdefiniowała jej ramy, a w latach kolejnych dokonała ich uporządkowania, osadzenia w ramach przyczynowo – skutkowych, wreszcie odniesienia do priorytetowej kwestii, którą jest spełnianie niezbędnych wymagań.

Cały czas ten zbiór wymagań charakteryzuje się uniwersalizmem, powszechną akceptacją, jak również elastycznością. Między innymi z tego powodu użytkownicy normy ISO 9001 urośli w siłę, która przekłada się na liczbę certyfikowanych na całym świecie systemów zarządzania jakością (ponad 1,3 miliona wydanych certyfikatów). Jednakże wypracowanie wspólnego języka wartości i jakości okazało się sprawą o tyle trudną, że skala stosowania wymagań normy jakościowej naraziła jej treści na nadinterpretacje lub niedointerpretowanie, a w konsekwencji na niezrozumienie i niepełne wykorzystanie tego narzędzia, przez organizacje je stosujące. Niezrozumienie istoty normy ISO 9001 przez wielu ją stosujących zagnało standard w kąt i zepchnęło do roli narzędzia marketingowego, umniejszając tym samym jej podstawowy cel – prewencję w zarządzaniu. Pomimo popełnienia takiego błędu przez liczne jednostki stosujące standard ISO 9001, ten nadal się broni. Dał bowiem w swoim zarysie początek normie ISO 27001. Jej twórcy, wykorzystując umiejętnie podejście procesowe oparte o cykl PDCA, rozpropagowane w ramach zarządzania jakością zrozumieli, iż nacisk na orientację względem klienta zewnętrznego nie jest jedynym gwarantem stabilności i jakości. Równie ważne jest zachowanie bezpieczeństwa informacji, danych, wiedzy i organizacyjnego know-how, szczególnie w czasach, gdy konkurowanie jakością wyrobu czy usługi, nie stanowi jedynego oczekiwanego modelu operacyjnego. Naturalnym w epoce, w której konkurencja opiera się na kapitale ludzkim, wydaje się zatem być wzmocnienie jakości poprzez zarządzanie bezpieczeństwem informacji.

> Systemy zarządzane są przez ludzi, a to właśnie czynnik ludzki jest najsłabszym ogniwem w bezpieczeństwie informacji.

Obecnie na rynku można zauważyć duże zainteresowanie normą ISO 27001 i bezpieczeństwem informacji. Co więcej organizacje posiadające dotychczas ISO 9001 decydują się na kolejny system i integrują obie normy ze sobą. Postawienie na jakość wytwarzanych produktów jest słusznym kierunkiem. Najważniejsza w procesie wytwarzania jest wiedza. Jak to zrobić? Gdzie kupić materiały? Jak korzystać z narzędzi? Jak sprzedać wytworzone produkty i komu? Jak ulepszyć produkt, aby był bardziej konkurencyjny? Itd. Dlatego też to informacja ma kluczowe znaczenie w nowoczesnych przedsiębiorstwach. Naturalną rzeczą jest więc jej ochrona. Na pytanie czy chronimy informacje większość z nas odpowiada że tak. Potrafimy powiedzieć jak ją chronimy i dlaczego. Mimo to ciągle słyszymy o nowych incydentach bezpieczeństwa informacji. Dzieje się tak z kilku powodów. Po pierwsze nie ma zabezpieczeń które w 100% uchronią nasze informacje. Wdrażając zabezpieczenia minimalizujemy ryzyko wystąpienia incydentu. Po drugie większość informacji występuje w wersji elektronicznej. Rozwój technologii z jednej strony ułatwia nam wdrażanie nowych zabezpieczeń, z drugiej stwarza nowe możliwości wycieku informacji. Po trzecie i najważniejsze – systemy zarządzane są przez ludzi, a to właśnie czynnik ludzki jest najsłabszym ogniwem w bezpieczeństwie informacji. Wróćmy jednak do tematu integracji systemów. Podstawową korzyścią takiej hybrydy jest wytwarzanie produktów odpowiedniej jakości przy jednoczesnym zabezpieczeniu wszelkich istotnych z punktu widzenia organizacji informacji przetwarzanych w firmie. Integracja systemów pozwala stworzyć wspólną dokumentację systemową oraz zmniejszyć czas i koszty związane z certyfikacją. Bezpieczeństwo informacji oparte jest na analizie ryzyka. Prawidłowe jej przeprowadzenie pozwala zdiagnozować słabe ogniwa i prawidłowo je zabezpieczyć. Oczywiście nie wszystkie zabezpieczenia wymienione w załączniku A normy trzeba wdrożyć. Dzięki analizie ryzyka możemy przyjąć pewne ryzyka jako akceptowalne. Dotyczy to sytuacji kiedy koszt wdrożenia zabezpieczenia jest większy niż zakładana przez nas strata związana z utratą poufności integralności lub dostępności informacji. Co jest najbardziej istotne nie dotyczy to kwestii prawnych. Są one chyba najsilniejszym

MAGAZYN INFORMATYKI ŚLEDCZEJ I BEZPIECZEŃSTWA IT

Adres redakcji
Mediarecovery
40-723 Katowice, ul. Piotrowicka 61
Tel. 32 782 95 95, fax 32 782 95 94
e-mail: redakcja@mediarecovery.pl

Redakcja
Sebastian Małycha (red. nacz.),
Przemysław Krejza
Skład, łamanie, grafika: Mariusz Ruski
Reklama: Damian Kowalczyk

Wydawca
Media Sp. z o.o.
40-723 Katowice, ul. Piotrowicka 61
Tel. 32 782 95 95, fax 32 782 95 94
e-mail: biuro@mediarecovery.pl

mediarecovery
Lider informatyki śledczej

i bezdyskusyjnym argumentem zarządzania bezpieczeństwem informacji. W naszym kraju obowiązuje wiele aktów prawnych związanych z ochroną pewnych informacji, do których stosować musi się każda organizacja. Są to np. rachunkowość, dane osobowe, informacja niejawna. Brak ochrony dla tych informacji może skutkować ciężkimi sankcjami finansowymi i karnymi zarówno dla organizacji jak i dla osób odpowiedzialnych za ich ochronę.

Poza prawnymi „powodami" wdrożenia normy ISO 27001 istotne są też wymagania klientów. Duże firmy posiadające wdrożony system i zabezpieczające informacje wewnątrz organizacji często korzystają z dostawców i przekazują im ważne z punktu widzenia analizy ryzyka informacje.

Trafiając do zewnętrznego podmiotu informacje te muszą być nadal skutecznie zabezpieczane. Pojawiło się również rozporządzenie, które nakłada na jednostki administracji publicznej wprowadzenie minimalnych zabezpieczeń dla systemów teleinformatycznych. Przy tej okazji po raz pierwszy norma ISO 27001 pojawiła się w akcie prawnym. Wdrożenie jej przez organizację skutkuje spełnieniem wymagań rozporządzenia.

Kierunki rozwoju obu standardów dają nadzieję na to, że systemy zarządzania oparte o wymagania ISO 9001 i ISO 27001 będą spójne, adekwatne dla potrzeb organizacji i jej partnerów biznesowych, oraz w jeszcze większym stopniu dopasowane do ryzyk, które ponoszą organizacje w dzisiejszym świecie.

Fenomen ISO 27001 oraz stabilna pozycja narzędzia jakościowego, którym jest ISO 9001 mogą ulec wzmocnieniu w najbliższym czasie. Już dziś klienci certyfikowani przez TUV NORD Polska podkreślają, że stosowanie rozwiązań systemowych, zawartych w normach 9001 i 27001 daje przede wszystkim korzyści wewnętrzne organizacji (badania wykonywane 8 – 10 lat temu pokazywały, iż certyfikowani uważają, że 80% systemu to korzyści marketingowe, obecnie ta proporcja przesunęła się w relacji 85/15 na rzecz korzyści dla stosującego).

Jeśli weźmie się pod uwagę, iż niedawno zakończony proces nowelizacji normy ISO 27001 i planowana na 2015 rok publikacja nowej wersji ISO 9001 mają te same cele i założenia – potencjalne korzyści wydają się znów zyskiwać na sile. Obie bowiem normy oparte o zarządzanie ryzykiem odniesionym odpowiednio do bezpieczeństwa informacji i do zarządzania jakością w procesach produkcyjnych, usługowych i zarządczych będą miały tą samą strukturę, możliwie zbieżną terminologię i układ wymagań, oparty o tak zwaną strukturę wyższego poziomu. Powodować to będzie ułatwienie w osiąganiu synergii pomiędzy jakością i bezpieczeństwem informacji. Łatwiejszym będzie wdrażanie i certyfikowanie zintegrowanych systemów jakości i bezpieczeństwa informacji. Tym samym będą one jeszcze czytelniejszymi i bardziej przyjaznymi narzędziami i zbiorami metod budowania wartości firm – zarówno wewnątrz, jak i w relacjach z otoczeniem zewnętrznym. Takie podejście i kierunki rozwoju obu standardów dają nadzieję na to, że systemy zarządzania oparte o wymagania ISO 9001 i ISO 27001 będą spójne, adekwatne dla potrzeb organizacji i jej partnerów biznesowych, oraz w jeszcze większym stopniu dopasowane do ryzyk, które ponoszą organizacje w dzisiejszym świecie.

Michał Gluska jest Product Managerem ds. Szkoleń Biznesowych w TUV NORD POLSKA Sp. z o.o.

Przemysław Szczurek jest Product Managerem ds. Bezpieczeństwa Informacji w TUV NORD POLSKA Sp. z o.o.