25 maja 2018 r. zacznie obowiązywać w Polsce Rozporządzenie o Ochronie Danych Osobowych (RODO, ang. GDPR). W jaki sposób podejść do tego tematu od strony działu IT? Bartłomiej Zadrożny – Key Account Manager w EIP i Karol Wróbel – Chief Technology Officer w 4SyncSolutions IT Security VAD, rozmawiali z redakcją ITwiz o bezpieczeństwie IT i narzędziach, które umożliwią przygotowanie się na zmiany.

Na jakie problemy wskazują klienci w kontekście RODO? Czy już interesują się tym tematem?

Bartłomiej Zadrożny (B.Z.): W większości są świadomi tego, że wchodzą nowe przepisy dotyczące bezpieczeństwa danych. Czasem jednak nie do końca wiedzą co zrobić i jak do tego podejść. Natomiast trzeba pamiętać, że RODO to nie tylko zagrożenia związane z ewentualnymi karami, lecz także szansa na sukces w dzisiejszych, cyfrowych czasach. RODO wymusza zwrócenie uwagi na kwestię bezpieczeństwa danych, na to w jaki sposób z nich korzystamy i jak nimi zarządzamy. Pozwala to nam na usprawnienie pewnych procesów w organizacji, a co za tym idzie – na poprawę biznesu i wizerunku w oczach klientów. Sami coraz częściej pod natłokiem globalizacji informacji możemy odczuć pewną frustrację, kiedy zweryfikujemy jak wiele da się znaleźć o nas samych, nawet niespecjalnie szukając. Wyobraźmy sobie więc co może osiągnąć specjalista, który będzie ukierunkowany tylko i wyłącznie na dane naszej firmy, a jego jedynym celem będzie zdobycie niewygodnych danych, czy dostępu do poufnych systemów. Taka osoba w przypadku sukcesu jest w stanie sparaliżować działanie firmy, a nawet doprowadzić ją do upadku.

Jak rozwiązania IT wspierają spełnienie wymogów związanych z RODO?

B.Z.: Wielu producentów stara się odnieść do tego tematu i wskazuje skuteczność swoich rozwiązań w zapewnieniu bezpieczeństwa na konkretnych poziomach. Należy jednak zwrócić uwagę na to, że każdy z nich musi być ze sobą zintegrowany. Z jednej strony zapewnienie pełnego bezpieczeństwa i zgodności z RODO jest związane z każdym z poziomów osobno, ale jednocześnie trzeba myśleć o nich wszystkich jako o jednym organizmie. Te poziomy to m.in. elementy infrastruktury oraz elementy systemowe, w tym sieci, usługi Active Directory, dostęp do systemów pamięci masowych, czy rozwiązania takie jak oferowana przez nas – a stworzona wspólnie przez Cisco i IBM – platforma VersaStack. Im większa integracja elementów infrastruktury IT, tym mniejsza ilość luk i błędów, które mogą być wykorzystywane przez cyberprzestępców.

Karol Wróbel (K.W.): Dostępne na rynku rozwiązania zapewniające bezpieczeństwo IT skupiają się głównie na ochronie przed zagrożeniami na styku naszej sieci z siecią publiczną. RODO koncentruje się zaś na ochronie danych. Z tego powodu każda organizacja powinna dokładnie zrozumieć schemat przepływu informacji – zarówno na styku sieci, jak i wewnątrz

niej. Dodatkowo w dużych organizacjach – z powodu mnogości systemów IT – specjaliści opiekujący się aplikacjami często nie mają pełnej świadomości co się dzieje z danymi, a nawet jakie i ile ich jest w firmie. Skoro nie wiemy, gdzie i jakie dane mamy, to jak można je chronić? Przy użyciu połączenia głębokiego dekodowania przesyłanej treści, pamięci sieciowej i zaawansowanych mechanizmów analitycznych systemu Fidelis Network, jesteśmy w stanie nie tylko zlokalizować miejsce przechowywania danych i przeanalizować ich przepływ na przestrzeni czasu, ale także zapobiec wyciekowi informacji dzięki funkcji blokowania. System Fidelis umożliwia przygotowanie się do zmian w systemach IT pod kątem wymagań RODO, a także pozwala weryfikować na przestrzeni czasu, czy ta zgodność jest zachowywana. Ponadto możemy rozpoznawać i blokować zaawansowane ataki na naszą infrastrukturę i użytkowników, których jedną z konsekwencji jest utrata danych.
Najważniejszą wartością dla klientów, jaką daje współpraca z EIP i 4SYNC, jest opracowanie kompleksowej strategii bezpieczeństwa organizacji, która pokrywa wszystkie kluczowe obszary.
Na czym polega współpraca pomiędzy EIP i 4SYNC w projektach związanych z RODO?
K.W.: Szukaliśmy partnera z wartością dodaną. Ważne były nie tylko kompetencje, specjalizacja, odpowiednie projektowanie rozwiązań, ale także utrzymanie ich po wdrożeniu. Powszechny problem firm – związany nie tylko z RODO, ale ogólnie z bezpieczeństwem IT – to brak odpowiednich specjalistów, którzy mogliby szybko zareagować na incydenty bezpieczeństwa IT. Połączenie kompetencji Fidelis, 4SYNC i EIP pozwala zaadresować ten problem.
B.Z.: Obszar bezpieczeństwa IT należy rozumieć szerzej. RODO nie jest jedynym elementem, który powinien motywować do dbałości o nie. W przeciwnym razie firma może ponieść znaczące straty z powodu włamania. Ucierpieć może jej renoma, a klienci mogą odejść. Rozwiązania Fidelis zapewniają zaś – obok zgodności z RODO – zabezpieczenie przed innymi działaniami przestępców. Ponadto rozwiązania te integrują się z komplementarnymi narzędziami zapewniającymi bezpieczeństwo IT, np. Next Generation Firewall. Naszym celem jest bowiem zapewnienie kompleksowego wsparcia i pomocy w zakresie cyberbezpieczeństwa. Oferujemy również dodatkową wiedzę, która pozwala przeprowadzić projekt kompleksowo, a po jego zakończeniu zapewnić wsparcie w zakresie wdrożonych narzędzi oraz dalszych, rozwojowych działań.
Jakie są najważniejsze funkcjonalności rozwiązania Fidelis w kontekście zapewnienia zgodności z RODO?
K.W.: Jednym z wymogów RODO jest zapewnienie ochrony adekwatnej do rodzaju i ilości

danych, które przetwarzamy. W związku z tym musimy być świadomi jakie dane przetwarzamy i gdzie, a także kto uzyskuje do nich dostęp. Rozwiązanie FidelisNetwork od 15 lat rozwijane jest jako specjalistyczne narzędzie do określenia przepływu informacji w sieciach firmowych. Przeprowadzana przez EIP wspólnie z 4SYNC analiza Proof of Concept – PoC– pomaga określić, jak dane przepływają i co należy poprawić w tym zakresie.
Fidelis „czyta" za nas całą komunikację sieciową – rozpoznaje treść przesyłanej informacji, klasy kuje ją, zapisuje dane śledcze związane z potencjalnymi naruszeniami i rozbudowany opis każdego najdrobniejszego elementu przesłanego w sieci. Monitorowanie odbywa się na wszystkich portach i protokołach, co pozwala na wykrywanie zagrożeń i wycieków danych nie tylko w standardowych kanałach komunikacji – web, mail, ftp, czy zasobach sieciowych, ale również w nietypowych kanałach komunikacyjnych, które atakujący wykorzystują do ukrywania swoich działań. Dzięki temu mamy do dyspozycji niespotykanie precyzyjny opis przepływu informacji, który jesteśmy w stanie dowolnie odtwarzać na przestrzeni wielu miesięcy wstecz.
Po analizie klient otrzymuje informacje m.in. o tym:
jak organizacja dzieli się danymi ze światem zewnętrznym;
jakiej klasy informacje wędrują na prywatne skrzynki pocztowe;
jak popularne jest korzystanie z dysków chmurowych;
czy w ten sposób przesyłane są dane klientów i tajemnice firmowe;
czy jakiekolwiek systemy w sieci zostały przejęte przez atakujących;
i w którym miejscu sieci skupić wysiłki w poprawie bezpieczeństwa.
Są to bezcenne informacje w kontekście zgodności z RODO.
Nasze narzędzia umożliwiają także projektowanie rozwiązań IT tak, aby od razu uwzględniały ochronę danych osobowych i wymogi RODO.
Kolejny etap to stały monitoring przepływu informacji, który pozwala szybko reagować na incydenty. Dzięki niemu można np. zablokować dostęp do informacji chronionej zarówno ze względu na zabronione działania użytkowników, jak i niepoprawnie funkcjonujące systemy IT. Fidelis pozwala przeszukiwać i wizualizować metadane o każdej sesji sieciowej, dokumencie, pliku i ich elementach składowych.
Fidelis oferuje też pełną analitykę, w tym tą dotyczącą incydentów związanych z bezpieczeństwem danych.
Nasze rozwiązanie – wykrywając takie zdarzenia – jest w stanie automatycznie na nie reagować i zapobiegać wyciekom danych. Jeśli jednak zrealizuje się najczarniejszy scenariusz i dojdzie do wycieku, Fidelis umożliwi zdecydowane przyspieszenie obsługi incydentu –

poprzez szybkie znajdowanie odpowiedzi na pytanie jakie dane, z jakich systemów wyciekły oraz czy miało to związek z atakiem na infrastrukturę, czy było wynikiem działań pracownika.

W jaki sposób rozpocząć przygotowania do wdrożenia RODO?

K.W.: Analiza PoC wskazuje, w jaki sposób zrealizować projekt, daje zalecenia, jak zabezpieczyć się przed potencjalnymi atakami i gdzie skupić wysiłki w dostosowywaniu obecnych systemów do nowych wymagań. To jest pierwszy krok na drodze do dostosowania się do tego rozporządzenia.

B.Z.: Najważniejszą rzeczą jest zweryfikowanie, jakie jest obecne podejście do bezpieczeństwa w organizacji. Dla jednych firm będzie to priorytet, a dla innych jedynie poboczna kwestia, do której nie przywiązują większej wagi. Oczywiście, jak wcześniej wspomniał Karol, sam w sobie PoC Fidelisa wskazuje nam jakie elementy wymagają analizy, ale by zapewnić szerszą perspektywę bezpieczeństwa, nie jest to wszystko, na co zwracamy uwagę. Aby odpowiednio przygotować się do wdrożenia rozwiązań, które spełniają wymogi RODO, należy przede wszystkim szczegółowo przeanalizować procesy, które są obecne w firmie, oraz zastanowić się, na jakich zasadach funkcjonują. Ogromne znaczenie mają tutaj prawa dostępu, które w dużych organizacjach często nie są uporządkowane, zarządzanie dokumentami i ich przesyłaniem, reguły postępowania w określonych przypadkach itp. Analizując to, możemy odpowiednio dobrać rozwiązania, które są w stanie rozwiązać pewne trudności i umożliwią podniesienie poziomu bezpieczeństwa.

Jak 4SYNC i EIP wspierają klientów we wdrożeniach?

B.Z.: Wykorzystując wiedzę i doświadczenie zespołów EIP i 4SYNC odpowiednio opracowujemy kompleksową strategię bezpieczeństwa, tak aby pokrywała wszystkie kluczowe obszary przedsiębiorstwa. Dotyczy to więc nie tylko przepływów danych, lecz także np. funkcjonowania aplikacji z bezpośrednim dostępem do internetu. Poza tym oferujemy audyt sprzętu. Trzeba bowiem wiedzieć, że jego złe podłączenie, błędne wykorzystanie oprogramowania do zarządzania nim może również narazić organizację na zagrożenie skutecznym atakiem cyberprzestępców. W związku z powyższym, po pierwsze, pomagamy określić, co może stanowić ryzyko dla bezpieczeństwa, a po drugie zminimalizować je poprzez odpowiednie zalecenia i rozwiązania wspierające ich realizację. Najważniejszy jednak w tym całym procesie ciągle jednak jest człowiek. Tak naprawdę organizacja nigdy nie będzie w stanie poprawić swojego poziomu bezpieczeństwa, jeżeli nie zaczną zwracać na nie uwagi wszyscy jej pracownicy, który mają jakikolwiek dostęp do systemów, łączy czy plików.

K.W.: Robiąc testy systemu Fidelis Network, tworząc analizy PoC, chcemy pokazać, jak wdrożyć oferowane rozwiązania, jak udoskonalić stosowane procedury i systemy IT w

konkretnej organizacji. Unikamy bowiem „pudełkowego” podejścia do bezpieczeństwa. Wdrażając platformę Fidelis, uzyskujemy narzędzia do kompleksowej analizy sieci i przepływu informacji, szybciej wykrywamy i blokujemy potencjalne zagrożenia, poprawiamy skuteczność obecnie wykorzystywanych rozwiązań bezpieczeństwa oraz możemy skutecznie i kompleksowo zabezpieczyć organizację.

Materiał został przygotowany na potrzeby raportu: “Wszystko co warto dziś wiedzieć o GDPR”, opracownym przez ITwiz.

Nowy raport: Wszystko co warto dziś wiedzieć o GDPR | ITwiz: Centrum Wiedzy o Bezpieczeństwie IT

Chcesz przetestować jak działa Fidelis Network? Napisz do nas: security@eip.pl