RODO

PARTNER TEMATU

esecure | SECUREVISIO

Przyszłość ochrony informacji

Wiedza to potęga

– Francis Bacon

Wraz z rozwojem nowoczesnej gospodarki opartej na skutecznej i szybkiej wymianie informacji, posiadanie i wydajne zarządzanie danymi jest nieodłącznym elementem działalności niemal każdej firmy. Nowe technologie komunikacyjne jak nigdy dotąd pozwoliły na rozszerzenie bazy potencjalnych klientów niemal na cały świat. Możliwości, jakie dają nam nowoczesne technologie znacząco zmieniły sposób komunikacji z klientem, jednocześnie zrodziły jednak nowe wyzwania dla firm szczególnie w dziedzinie ochrony ich danych personalnych.

Dotychczas przepisy prawne często „nie nadążały" za nieustannie postępującymi zmianami w technologii. Zrodziło to potrzebę ujednolicenia przepisów oraz powstanie ogólnego rozporządzenia o ochronie danych osobowych (RODO). Rozporządzenie zaczynie obowiązywać 25 maja 2018 r., co pozostawia niewiele czasu na przygotowanie się.

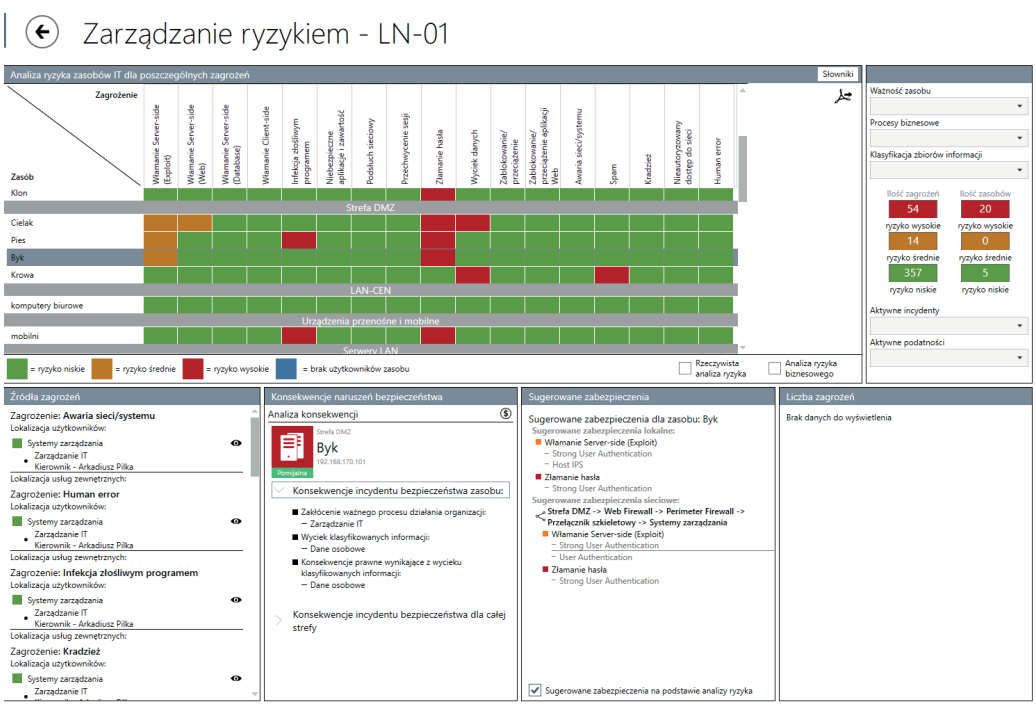
Nowe koszty

Za naruszenie przepisów GDPR (General Data Protection Regulation) dotyczących obowiązków administratora i podmiotu przetwarzającego grożą kary w wysokości do 10 mln euro lub do 2% całkowitego rocznego światowego obrotu przedsiębiorstwa (art. 83 pkt 4). Zaś za naruszenie m.in.: podstawowych zasad przetwarzania, praw osób, których dane dotyczą lub przekazywania danych osobowych do państwa trzeciego grożą kary już dwukrotnie wyższe. Potencjalne koszty, jakie może generować zaniedbanie bezpieczeństwa danych są więc ogromne!

Nowe prawo

Jedną z kluczowych kwestii, na których opiera się rozporządzenie jest zasada rozliczalności. W tym przypadku polega ona na wdrożeniu środków gwarantujących przestrzeganie przepisów w związku z operacjami przetwarzania oraz posiadanie dokumentacji wskazującej, jakie działania podjęto, aby zapewnić przestrzeganie przepisów rozporządzenia. Aspekt ten narzuca wymóg posiadania odpowiednio ustrukturowanego systemu do zarządzania i dokumentowania bezpieczeństwa zarówno danych osobowych, jak i całej firmy. Wyzwania związane z zapewnieniem bezpieczeństwa tak kluczowych i skonsolidowanych danych firm, wraz z czasochłonnym procesem ich gromadzenia i przetwarzania, zmotywowały nas do stworzenia programu SecureVisio. Jest to nowoczesne rozwiązanie typu Real Time GRC (Governance, Risk Management, Compliance) pozwalające na automatyzację wielu złożonych oraz czasochłonnych procesów związanych z zarządzaniem bezpieczeństwem oraz tworzeniem i utrzymywaniem dokumentacji. Wielokrotnie w treści rozporządzenia podkreślane jest jak ważnym elementem ochrony danych jest posiadanie odpowiedniej analizy ryzyka podczas przetwarzania danych. Między innymi art. 35 wprowadza wymóg przeprowadzenia oceny skutków przetwarzania, *„Jeżeli dany rodzaj przetwarzania […] może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków […] przetwarzania dla ochrony danych osobowych"* – czytamy w nim. Oznacza to że administrator musi przed podjęciem działań określić jakie ryzyko wiąże się z każdą podjętą przez niego akcją. Ocena ryzyka wspomniana w art. 35 musi zawierać m.in. opis oraz cele planowanych operacji przetwa-

1. Analiza ryzyka



rzania, ocenę ryzyka naruszenia praw osób, których dane dotyczą oraz środki zastosowane w celu zarządzania ryzykiem. Tak skonstruowane prawo nakłada na administratora znacznie więcej obowiązków niż wynika to bezpośrednio z potrzeb zarządzania danymi. System planowania oraz zarządzania ryzykiem, taki jak SecureVisio, jest więc niezbędny do prawidłowej pracy. Aby dodatkowo usprawnić pracę, SecureVisio aktywnie wspomaga redukcje ryzyka, m. in. poprzez sugerowanie zabezpieczeń zwiększających bezpieczeństwo przetwarzania danych.

Na **1.** przedstawiona została przykładowa analiza ryzyka wykonana w SecureVisio.

Dodatkowo art. 30 nakłada na administratora obowiązek prowadzenia rejestru czynności przetwarzania, w którym znajdować się mają informacje dotyczące celu i zakresu przetwarzania, kategorii odbiorców oraz osób, których dane dotyczą, dane administratora oraz opis technicznych i organizacyjnych środków bezpieczeństwa. Dodatkowo, zgromadzone w ramach prowadzonego rejestru informacje powinny być udostępniane organowi nadzorczemu w przypadku kontroli. Rejestr taki musi więc być aktualny oraz łatwo dostępny i czytelny. SecureVisio spełnia rygorystyczne kryteria bezpieczeństwa przy jednoczesnym przejrzystym dostępie dla audytorów.

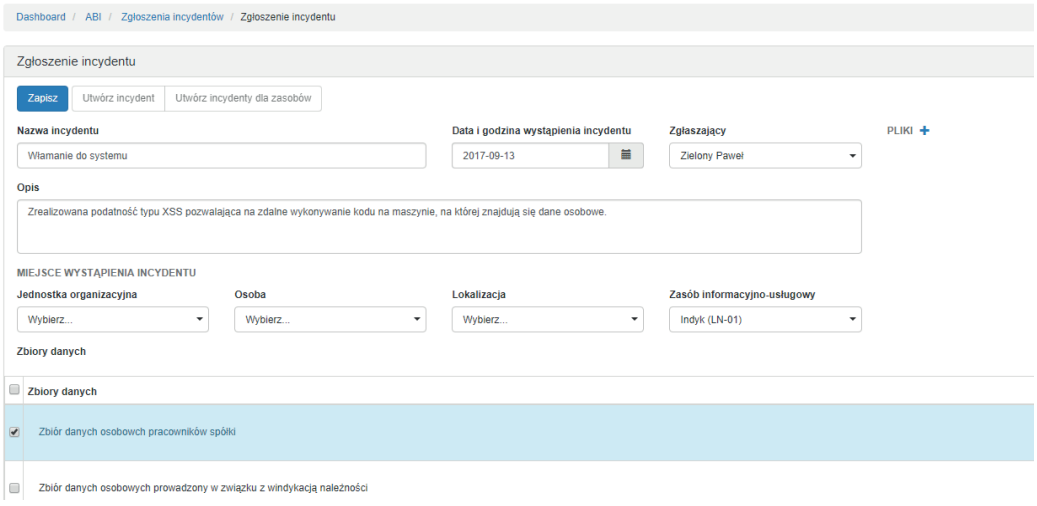
Kolejnym ważnym aspektem są prawa przysługujące osobom, których dane dotyczą oraz ich egzekwowanie. Osoba taka ma prawo m.in. do wglądu w swoje dane, ich korektę, przeniesienie lub całkowite usunięcie. Ma również możliwość wycofania zgody na przetwarzanie swoich danych. Pojawia się zatem potrzeba posiadania odpowiednich systemów zarządzania i obsługi tego typu wniosków, zwłaszcza przy „prawie do bycia zapomnianym" (art. 17) lub cofnięciu zgody na przetwarzanie danych, gdyż mogą istnieć inne przesłanki prawne dalszego ich przetwarzania. Rozwiązania tego typu powinny umożliwić sprawne oraz rzetelne przetwarzanie wniosków. By usprawnić ten proces, SecureVisio posiada specjalny moduł odpowiedzialny za obsługę i przetwarzanie wniosków.

Ponadto *„Administrator dokumentuje […] okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorczemu weryfikowanie przestrzegania niniejszego artykułu"* (art. 33 pkt. 5).

W świetle przepisów RODO obowiązek zgłaszania incydentów bezpieczeństwa mają nie tylko firmy telekomunikacyjne, tak jak to było dotychczas, ale wszystkie podmioty przetwarzające dane osobowe. W przypadku naruszenia administrator ma 72 godziny na jego zgłoszenie. Bardzo ważną kwestią jest w tym wypadku czas, sprawność procedury zgłaszania i monitorowania incydentów. Elementy te mogą zaważyć na późniejszej decyzji organu nadzorczego, czy doszło do naruszenia rozporządzenia oraz w jakim stopniu wykazana została zgodność z GDPR.

Na **2.** przedstawiony został system zgłaszania incydentów w SecureVisio.

2. Zgłoszenie incydentu w SecureVisio



Nowe rozwiązania

Przedstawione powyżej aspekty GDPR tworzą przejrzysty obraz wymagań stawianych przed administratorami. Wyzwaniem przy spełnianiu norm zawartych w RODO jest nie tylko zachowanie najwyższych standardów bezpieczeństwa, ale również klarowności dla organów nadzorczych. Nakłada to znacznie więcej obowiązków na firmy i administratorów danych. W celu spełnienia wymagań rozporządzenia GDPR, przy jednoczesnym zminimalizowaniu nakładu pracy i kosztów, program SecureVisio stosuje wielopoziomowe rozwiązania odnoszące się do niemal wszystkich aspektów zawartych w nowych zasadach administracji danymi przy jednoczesnym zachowaniu intuicyjnego interfejsu oraz wspomaganiu administratora poprzez automatyzację procesów zarządzania danymi osobowymi. SecureVisio pozwala na wejście pewnym krokiem w przyszłość administracji danych, a jego kompleksowość umożliwia zaadresowanie wymagań rozporządzenia. ■

Więcej na: www.securevisio.pl
Kontakt: Ewa Pasewicz,
ewa.pasewicz@esecure.pl