GDPR w praktyce - systemy uwierzytelniania

Co to jest GDPR?

Zgodnie z przyjętym przez instytucje Unii Europejskiej kalendarzem w maju 2018. roku zaczną obowiązywać nowe przepisy dotyczące ochrony danych osobowych. Ich zakres jest określony rozporządzeniem o nazwie "General Data Protection Regulation" - GDPR - (1). Rozporządzenie GDPR precyzuje zasady administrowania danymi osobowymi oraz określa konsekwencje wynikające z niezastosowania się do nich. Wprowadzenie GDPR powoduje, że firmy muszą gruntownie zweryfikować wewnętrzne procesy dotyczące bezpieczeństwa przetwarzanych przez nie danych osobowych.

Wszystkie organizacje przetwarzające dane osobowe w sposób automatyczny podlegać będą GDPR – od niewielkich sklepów online, poprzez sieci handlowe prowadzące programy lojalnościowe, aż do międzynarodych gigantów rynku internetowego. Nowe przepisy w zakresie ochrony danych osobowych będą obowiązywały każdą firmę i organizację, która przetwarza dane osób, a więc np: apteki, uczelnie, towarzystwa ubezpieczeniowe czy banki. Aby nie narazić się na sankcje związane z niezgodnością z GDPR, organizacje muszą w pełni kontrolować składowanie i przetwarzanie danych, tj.: wiedzieć, gdzie dane są przechowywane, dokąd migrują, komu są udostępniane, jakie zgody zostały udzielone i wreszcie - dysponować procedurami trwałego usuwania danych osobowych.

GDPR w praktyce

GDPR składa się z 99 artykułów, z których tylko 6 bezpośrednio odnosi się do bezpieczeństwa teleinformatycznego. W GDPR punktem wyjścia do planowania bezpieczeństwa jest artykuł 35 i analiza ryzyka – dla danych osobowych określana terminem oceny skutków dla ochrony danych (Data protection impact assessment).

GDPR a kontrola dostępu

Na szczęście ogólne obszary ryzyka w przetwarzaniu danych osobowych oraz sposoby jego redukcji w systemach IT zostały dobrze opisane, rozpoznane są też techniczne metody jego eliminacji. Musimy pamiętać, że pierwszym krokiem wdrażania procedur zgodności z GDPR jest rozpoznanie: procesów, systemów przetwarzających i przechowujących dane osobowe. Jednocześnie, po wykonaniu analizy wdrożenie odpowiednich zabezpieczeń nie jest trudne, gdyż istnieją powtarzalne schematy wdrażania systemów ochrony.

Jednym z podstawowych obszarów ryzyka jest brak kontroli dostępu, dotyczy to zarówno dostępu do systemów przetwarzających dane osobowe, jak i systemów bazowych i pomocnicznych. Przykładowo - nie wystarczająco bezpieczny system uwierzytelniania oparty na statycznych hasłach przechowywanych w Active Directory naraża na szwank wszystkie środowiska IT firmy - w tym te odpowiedzialne za dane osobowe.

Autoryzacja 2FA

Na szczególne ryzyko narażone są systemy "stykające" się ze światem zewnętrznym - tj. systemy zdalnego dostępu VPN, poczta elektroniczna, systemy wymiany plików, itp. Powszechnie uznaje się, że właściwą metodą kontroli dostępu jest autoryzacja użytkowników bazująca na modelu 2FA (Two Factor Authentication), a więc zazwyczaj na czymś, co użytkownik zna (hasło) i na czymś, co posiada (token uwierzytelniający, smartfon, lista haseł jednorazowych, itd.). Z przyczyn praktycznych, najczęściej stosowane są systemy 2FA bazujące na tokenach PKI (z portem USB, przechowujące certyfikat lub karty stykowe), tokeny OTP (generujące hasła jednorazowe na wyświetlaczu LCD) oraz tokeny wirtualne w postaci apikacji na smartfonie.

ul. Rakowiecka 36
02-532 Warszawa
tel. +48 22 646-68-73
fax +48 22 606-37-80
e-mail: office@cc.com.pl
Web: http://www.cc.com.pl/

CC Otwarte Systemy Komputerowe Sp. z o.o. zarejestrowana w Wydz.XIII Gospodarczym KRS, pod nr 0000023570, zarząd: Grzegorz Blinowski – Prezes Zarządu, Tomasz Ramsza - Członek Zarządu; Kapitał zak.:100000 PLN

Wdrożenie autoryzacji 2FA

Wdrożenie autoryzacji 2FA (2) przez wiele lat uchodziło za kosztowne, czasochłonne i technicznie trudne. Po części jest to prawda - system 2FA w zależnosci od przyjętego rozwiązania wymaga dedykowanego serwera autoryzacyjnego (AAA - najczęściej zgodnego z RADIUS), urzędu certyfikacji PKI, systemu zarządzania tokenami/kartami, itp. Obecnie, dzięki rozwiązaniom SaaS (Software as a Service) wdrożenie autoryzacji 2FA bardzo się uprościło: użytkownicy otrzymują tokeny fizyczne lub instalują aplikację na smartfonie, administrator konfiguruje reguły dostępu i przeprowadza integrację systemu autoryzacji z firewallem lub bramką VPN, jednak cały system autoryzacji znajduje się na serwerach chmurowych. Dzięki temu firma posiada kontrolę administracyjną nad dostępem użytkowników, nie ponosi jednak kosztów amortyzacji i eksploatacji serwerów uwierzytelniających.

System autoryzacji SAS firmy Gemalto

System autoryzacji Gemalto funkcjonuje w modelu SaaS. Integruje się ze wszystkimi popularnymi systemami firewall i bramkami zdalnego dostępu (np. CheckPoint, CISCO, Fortinet, Juniper, Microsoft, PaloAltoNetworks i innymi). W ramach zakupionej licencji otrzymujemy pakiet autoryzacyjny na określoną liczbę użytkowników, w którym możemy wykorzystywać różne fizyczne metody autoryzacji. Przykładowo: przy zakupie licencji na 50 użytkowników możemy otrzymać 20 tokenów OTP, 20 licencji na wirtualny token komórkowy, a 10 licencji zachować "w odwodzie" do dalszej decyzji. Cena pakietu jest stała i niezależna od typu i liczby wybranych autentykatorów (OTP, tokeny-wirtualne, tokeny e-mail).

(1) https://www.eugdpr.org/
(2) "Rozwiązania w zakresie autoryzacji OTP"; Opracowanie własne CC, styczeń 2018

ul. Rakowiecka 36
02-532 Warszawa
tel. +48 22 646-68-73
fax +48 22 606-37-80
e-mail: office@cc.com.pl
Web: http://www.cc.com.pl/