GDPR w praktyce - jak przygotować systemy IT do spełnienia nowych wymagań UE?

Co to jest GDPR?

Zgodnie z przyjętym przez instytucje Unii Europejskiej kalendarzem, w maju 2018 roku zaczną funkcjonować 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 znacznie zwiększa kary za naruszenia prywatności. Rozporządzenia będą egzekwowane od maja 2018 r. we wszystkich przedsiębiorstwach na świecie, które obsługują dane dotyczące osób UE. Zgodnie z wytycznymi dla "ISSA Journal" dotyczącymi zgodności z GDPR w zakresie doboru narzędzi kontroli bezpieczeństwa możemy podzielić przygotowania do wdrożenia zgodności z ustawą na 3 etapy:

1. Identyfikacja i lokalizacja wszystkich zbiorów przetwarzanych danych osobowych – aby chronić dane potrzebujemy wiedzieć gdzie się znajdują.

2. Implementacja kontroli dostępu do danych osobowych – żeby chronić dane potrzebujemy wiedzieć kto ma prawo dostępu.

3. Identyfikacja i zarządzanie ryzykiem – żeby chronić dane potrzebujemy wiedzieć, czy dostęp jest właściwie chroniony i szybko reagować na incydenty.

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. Omówmy pokrótce dostępność różnych narzędzi komercyjnych dla w.w. trzech obszarach:

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

I. Lokalizacja i identyfikacja danych

Ten zakres czynności w dużej mierze musi być wykonany "ręcznie", poprzez analizę dokumentacji, a jeśli jest to niezbędne, audyt przeprowadzony przez wyspecjalizowaną firmę. W obszarze tym dysponujemy jednak także przydatnymi narzędziami IT, do których należą:

1. Elektroniczne systemy dokumentacji zasobów IT
2. Systemy DAS (Discovery and Assessment).
3. Systemy DLP (Data Leakage Prevention, tj. zapobiegające wyciekowi danych) - niektóre z nich posiadają moduły automatycznej lokalizacji i rozpoznania źródeł i zbiorów danych.

Warto zapoznać się tu z ofertą takich producentów jak: Secure Vision (1), Imperva (2), Forcepoint (3).

II. Implementacja kontroli dostępu

Kontrolę dostępu w kontekście GDPR rozumiemy bardzo szeroko - zarówno w aspekcie zabezpieczenia przed próbami włamania jak i nieautyzowanego dostępu z wnętrza organizacji, w tym obszarze dysponujemy następującymi rodzajami narzędzi IT:

1. NGFW (Next Generation Firewall)
2. Systemy zarządzania i kontroli, w tym autoryzacji 2FA dla dostępu zdalnego
3. Systemy DLP (Data Loss Prevention)
4. Systemy WAF (Web Application Firewall) oraz DBF (Database Firewall)
5. Rozwiązania klasy MDM/EMM (enterprise Mobility Management)
6. systemy ochrony dostępu uprzywilejowanego (CyberArk)

W obszarze tym warto zapoznać się z ofertą takich producentów jak: CheckPoint, Palo Alto Networks i Juniper Networks (1); Gemalto, PulseSecure, ActivIdentity (2); Palo Alto Networks, Forcepoint (3); Imperva (4); Mobile Iron (5) oraz Wheel (6).

III. Identyfikacja i zarządzanie ryzykiem

W ramach tego obszaru możemy posłużyć się następującymi rozwiązaniami komercyjnymi:

1. Systemy wykrywające intruzów w sieciach i bazach danych.
2. Systemy SIEM.
3. Systemy do zarządzania podatnościami.
4. Systemy do priorytezacji incydentów i podatności.

W obszarze tym warto zapoznać się z ofertą takich producentów jak: Exabeam, Forcepoint, Flowmon, McAffee; AlienVault, EiQ NETWORKS, Juniper; Greenbone, Rapid7, Tenable; SecureVisio.

(1) https://www.eugdpr.org/