MAJ 2019

RAPORT interaktywnie.com

RODO I CYBERBEZPIECZEŃSTWO

POD PATRONATEM:

WP interia onet BUSINESS INSIDER POLSKA GAZETA.PL

SPIS TREŚCI

Uważaj na cyberataki, swoich pracowników i przepisy prawne

Jak pokazują badania, najwięcej firm, bo około jedna trzecia, doświadczyło w ubiegłym roku od jednego do trzech cyberataków. 21 procent twierdzi, że odnotowała ich od 4 do 9, a 6 procent podmiotów, że zostały zaatakowane co najmniej 30 razy w ciągu dwunastu miesięcy. Często powodowało to wielomilionowe straty.

Zdecydowana większość firm nie ma jednak zatrudnionych specjalistów od cyberbezpieczeństwa czy nawet RODO. Fakt, nie wszystkie muszą. Można i warto takie zadania powierzyć przecież profesjonalistom. Ale i oni nie załatwią wszystkich problemów, bo najsłabszym ogniwem każdej firmy są... jej pracownicy, którzy instalują programy na służbowych komputerach, korzystają z rozmaitych aplikacji na smartfonach, otwierają podejrzane maile itp., itd.

Roześlijcie im więc proszę ten plik pdf – raport Interaktywnie.com o RODO i cyberbezpieczeństwie. To podstawowe kompendium wiedzy, które przyda się praktycznie w każdym dziale przedsiębiorstwa, a przede wszystkim w marketingu.

Zapraszam do lektury

Tomasz Bonek, prezes zarządu i redaktor naczelny Interaktywnie.com

WIZYTÓWKI FIRM

inCV.pl

Adres
ul. Sienkiewicza 22
60-818 Poznań

Dane kontaktowe
E-mail: kontakt@incv.pl
Strona www: www.incv.pl
Telefon: 61 847 40 07

Opis działalności
inCV to narzędzie do otrzymywania, przechowywania oraz zarządzania CV kandydatów we wszystkich procesach rekrutacyjnych w Twojej firmie.

InCV to:
- tworzenie rekrutacji na nowe stanowiska
- bezpieczne udostępnianie CV
- automatyczne usuwanie danych osobowych po określonym terminie
- możliwość wysyłania wiadomości do kandydatów i komunikacja z nimi
- możliwość dodawania komentarzy do CV kandydatów

Wybrani klienci
Grupa Krotoski-Cichy, Volkswagen Group Polska, Globe Group, B2Net, Globe System,

Sinersio Polska Sp. z o.o.

Adres
ul. Inżynierska 8
67-100 Nowa Sól

Dane kontaktowe
E-mail: office@sinersio.com, sprzedaz@sinersio.com
Strona www: sinersio.com
Telefon: +48 68 411 44 40, +48 68 411 44 52

Opis działalności
Oferujemy usługę chmury obliczeniowej Sinersio Cloud w modelu IaaS. Doradzamy w zakresie doboru infrastruktury IT pod projekty biznesowe. Specjalizujemy się w hostingu systemów ERP, CRM, WMS, DMS i innych branżowych. Posiadamy własne, bezpieczne i niezawodne data center. Zapewniamy ciągłość działania i wsparcie techniczne w trybie 24/7/365.

Wybrani klienci
Pako Lorente, Kaczmarek Electric S.A., Ekoenergetyka, Piotr i Paweł, Elektrociepłownia Andrychów, PaulaFish, Narodowe Centrum Badań i Rozwoju (NCBiR), Naukowa i Akademicka Sieć Komputerowa Państwowy Instytut Badawczy (NASK PIB).

KTO MUSI WDROŻYĆ I STOSOWAĆ RODO

Kaja Grzybowska
redaktor Interaktywnie.com

kg@interaktywnie.com

1

RODO, czyli Rozporządzenie Ogólne o Ochronie Danych Osobowych (z ang. GDPR, czyli General Data Protection Regulation), rok temu wywoływało panikę przedsiębiorców, przerażonych wizją astronomicznych kar, jakie grożą za nieprawidłowości. Można już stwierdzić, że rzeczywistość nie jest tak straszna jak prognozowano, mimo że zasady gry na rynku danych rzeczywiście znacznie się zmieniły.

RODO.
Przeczytaj całą treść Rozporządzenia.

RODO weszło w życie już 24 maja 2016 roku, ale dopiero od 25 maja 2018 roku jego przepisy zaczęły obowiązywać i widmo kar - a mogą sięgać nawet 20 mln euro lub 4% obrotu z poprzedniego roku - stało się realnym zagrożeniem. Wszyscy też zrozumieli, że - mimo nagłaśniania głównie związanych z RODO absurdów przepisy Rozporządzenia trzeba traktować poważnie.

Za pierwszy przykład posłużyła Portugalia, której organ nadzorczy w tym kraju - Comissão Nacional de Proteção de Dados (CNPD) - nałożył karę w wysokości 400 tys. euro na szpital w Barreiro Montijo. Za nią poszły następne państwa. W Austrii zdecydowano o nałożeniu kary w wysokości 4800 euro za źle umiejscowiony monitoring.

W Stuttgarcie komisarz ds. Ochrony danych osobowych dla Niemieckiego kraju związkowego Badenia-Wirtembergia Stefan Brink poinformował **o nałożeniu na sieć społecznościową Knuddels grzywny w wysokości 20 000 euro. Powodem nałożenia kary było nieprawidłowe przechowywanie haseł użytkowników, a dokładniej brak mechanizmów szyfrowania danych.** Niemiecki urząd uznał, że firma z Karlsruhe naruszyła obowiązek zapewnienia bezpieczeństwa danych osobowych.

W Polsce pierwszą karę UODO wymierzył w marcu 2019 za niedopełnienie obowiązku informacyjnego. Firma, która przetwarzała w celach marketingowych dane pozyskane

Takie linki, że aż liny

Wzmocnij swoje SEO. Wykorzystaj potencjał serwisów odwiedzanych przez przeszło 20 mln internautów.

semahead

ze źródeł publicznie dostępnych, m.in. z Centralnej Ewidencji i Informacji Działalności Gospodarczej (CEiDG), musi zapłacić ponad 943 tys. UODO uznał bowiem, że powinna ona poinformować wszystkich (poinformowała jedynie tych, do których miała kontakt mailowy) właścicieli danych o ich przetwarzaniu i nie ma znaczenia fakt, że były one wcześniej dostępne w ogólnych bazach. Brak takiej informacji oznaczał, że bardzo wiele osób zostało pozbawionych możliwości skorzystania z przysługujących im praw. Nie mogły np. sprzeciwić się dalszemu przetwarzaniu, żądać sprostowania albo nawet ich całkowitego usunięcia.

> Według Europejskiej Rady Ochrony Danych złożono ponad 42 tys. skarg do krajowych organów nadzorczych (w Polsce prawie 2 500 skarg do Prezesa Urzędu Ochrony Danych Osobowych).
>
> *źródło: komunikat ODO 24 | Interaktywnie.com*

Na wysokość kary wpłynął fakt, że firma zdawała sobie sprawę z niedopatrzenia, ale nie podjęła działań zmierzających do naprawienia szkody. Postawa administratorów miała niebagatelne znaczenie dla UODO także w przypadku drugiej sprawy, która dotyczyła jednego ze związków sportowych. Udostępnił on na stronie internetowej dane sędziów (w tym ich adresy i numery PESEL), zdając sobie sprawę, że to niedozwolone działanie. Przez pół roku nie zrobił jednak nic, by naprawić błąd.

Czym jest unijne rozporządzenie o ochronie danych osobowych i jak należy je stosować?

Ogólną ideą stojącą za wprowadzeniem Rozporządzenia jest przywrócenie kontroli nad danymi ich właścicielom, czyli obywatelom. RODO przyznaje im prawo m.in do:

- przeniesienia danych;
- wglądu i dostępu do swoich danych;
- ich usunięcia („Prawo do bycia zapomnianym").

Tym samym nakłada na firmy przetwarzające dane obowiązek wprowadzenia procedur, które domyślnie będą nastawione na ich ochronę (privacy by design i privacy by default).

W praktyce oznacza to, że proces przetwarzania ma być zaprojektowany tak, żeby maksymalnie zredukować ryzyko ewentualnych wycieków, co wiąże się też z obowiązkiem rejestrowania poszczególnych czynności i etapów przetwarzania, a także wyznaczeniem osób, które będą za nie odpowiedzialne.

Tylko wtedy obywatele będą mieli gwarancję, że w każdej chwili i bez zbędnej zwłoki będą mogli skorzystać z np. prawa do bycia zapomnianym. W innym przypadku, kiedy nie wiadomo kto, co i po co przetwarza, byłoby to niewykonalne. Firmy muszą więc wykorzystywane dane (także te, które zebrane zostały przed wprowadzeniem RODO) zlokalizować i stworzyć techniczne zaplecze, które będzie umożliwiło ich skuteczne wyczyszczenie.

RODO nie precyzuje krok po kroku, jak modelowy proces przetwarzania powinien wyglądać. Zobowiązuje jedynie do **„adekwatnej"** ochrony powierzonych danych.

Jak RODO wpłynęło na działania marketingowe

RODO określa, że przedsiębiorca może przetwarzać tylko te informacje, które są niezbędne do świadczenia usług klientom, co wyklucza zbieranie danych „na zapas". Dane można więc przetwarzać w minimalnym zakresie, zarówno jeśli chodzi o ich zakres, jak i czas ich przechowywania. Zmieniło się więc dużo, jeśli chodzi o tzw. profilowanie. Wykorzystywanie danych, które do tej pory mogły być agregowane i używane np. do lepszego dopasowywania ofert bez wiedzy klienta, teraz jest uzależnione od jego zgody. Ale to tylko jedno z wielu wyzwań.

W cyfrowej rzeczywistości, która w dużej mierze żyje z danych, początkowo trudno było nawet zdefiniować, czym są dane osobowe i czy w związku z tym pliki cookies też podlegają ochronie. Odpowiadają co prawda za śledzące nas reklamy, ale przecież nie umożliwiają identyfikacji z imienia i nazwiska… Wątpliwości, na łamach Interaktywnie.com rozwiała, Agnieszka Świątek-Druś, rzecznik prasowy Urzędu Ochrony Danych Osobowych, stwierdzając, że:

- Plik cookies należy uznać za daną osobową, jeśli inne okoliczności, takie jak: czas, miejsce, w którym został on zapisany, lub jego zawartość z dużym prawdopodobieństwem umożliwiają identyfikację osoby, której dotyczy.

Poważne potraktowanie kwestii własności danych wymusiło na przedsiębiorcach - nie tylko internetowych - zmianę w myśleniu o relacji z klientem. RODO zmusiło ich do tego, by - po pierwsze - jasno informowali klientów o swoich działaniach, a - po drugie - by robili to w sposób, który zapewni ich przychylność. Ostatecznie klient może, ale nie musi zgodzić się na przetwarzanie swoich danych, trzeba więc go przekonać.

Regulaminy e-sklepów w większości musiały zostać przetłumaczone z prawniczego na język powszechny, a tzw. checkboksy, które zaznaczaliśmy celem udzielenia niezbędnych zgód, nie mogły być już domyślnie odhaczone na „tak".

Ochronie podlegają jednak nie tylko dane, które przekazujemy sklepom podczas zakupów, ale także te zawarte w korespondencji mailowej i systemach marketing automation. By realizować

Czy udzielenie agencji marketingowej dostępu do plików cookies jest powierzeniem danych osobowych?

Udzielenie innemu podmiotowi dostępu do zarządzanych przez nas danych osobowych lub danych umożliwiających identyfikację osób, których one dotyczą, zebranych za pomocą innych narzędzi, należy uznać za powierzenie przetwarzania.

Każde powierzenie przetwarzania danych, zgodnie z art. 28 ust. 3 RODO, może być realizowane wyłącznie na podstawie umowy lub innego instrumentu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego i wiążą podmiot przetwarzający i administratora, określają przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, a także obowiązki i prawa administratora.

Czy nadanie agencji marketingowej dostępu do Google Analytics jest powierzeniem przetwarzania danych osobowych?

W kontekście Google Analytics należy mieć na uwadze, że nie zawsze będzie dochodziło do przetwarzania danych osobowych, gdyż nie zawsze Google Analytics wykorzystuje pełne adresy IP komputerów, z których pobiera informacje. O przetwarzaniu danych osobowych w kontekście Google Analytics w pełnym zakresie nie można mówić np. wówczas, jeśli administrator, włączając Google Analytics, użył funkcji _anonymizeip, która na najwcześniejszym etapie zbierania danych anonimizuje użytkownika, zastępując ostatni oktet adresu IP jego urządzenia zerami.

Kiedy identyfikator internetowy staje się daną osobową?

Zgodnie z motywem 30 preambuły do RODO, identyfikatory internetowe – takie jak adresy IP, identyfikatory plików cookie – generowane przez ich urządzenia, aplikacje, narzędzia i protokoły, czy też inne identyfikatory, generowane na przykład przez etykiety RFID należy uznać za dane osobowe, jeśli czas, miejsce i kontekst, w którym one się pojawią w połączeniu z unikatowymi identyfikatorami i innymi informacjami dostępnymi w systemie informatycznym mogą być wykorzystywane do zidentyfikowania osób, których one dotyczą.

Agnieszka Świątek-Druś
rzecznik prasowy Urzędu Ochrony Danych Osobowych

źródło: Interaktywnie.com

obowiązki wynikające z RODO zgodnie z wymogami, konieczne stało się sprawdzenie, jak radzą sobie w tym zakresie dostawcy naszego oprogramowania, choć na tym polu, zwłaszcza ci najbardziej znani, raczej nie pozwalali sobie na nonszalancję.

RODO w HR

Zmiany przepisów związanych z ochroną danych osobowych dotyczą również działów HR, które co dzień zarządzają danymi wszystkich - przyszłych i obecnych - pracowników.

Informacje, które trafiają na biurka HR-owców - tak samo jak wszystkie inne - podlegają zwiększonej ochronie i zamknięcie nadesłanych CV na klucz w szufladzie nie wystarczy, by za taką ją uznać. W sukurs HR-owcom idą więc techniczne rozwiązania, które dają możliwość pseudonimizacji, anonimizacji czy szyfrowania danych osobowych i zapewniają odpowiedni poziom integralności systemu ich przechowywania.

Zakres danych, jakiego pracodawca może od nas żądać pozostaje bez zmian, ale - co ważne - nie można już uzależniać od nich wykonania umowy (jeśli przetwarzanie danych osobowych nie jest niezbędne do jej wykonania). RODO wprowadza też całkowity zakaz przetwarzania przez pracodawcę danych wrażliwych, dotyczących: nałogów, stanu zdrowia czy orientacji seksualnej a w przypadku, gdy dane przekazywane są zewnętrznym agencjom rekrutacyjnym konieczne staje się

udostępnienie informacji o tym, kto, kiedy i w jaki sposób będzie miał do nich dostęp.

Jak uniknąć kary za niedopatrzenia związane z RODO?

RODO nie precyzuje, co uważane jest za adekwatny poziom ochrony danych, więc tym bardziej, nie może precyzować, jak zorganizować procesy ich przetwarzania ani jakich technologii w tym celu użyć. Dla polskich przedsiębiorców, którzy w dobrą wolę urzędników nie ufają, to duże wyzwanie.

Każda firma inaczej jednak przetwarza informacje, musi więc indywidualnie oszacować ryzyko i dopasować do niego odpowiednie procedury. Inne powinny obowiązywać lokalny salon fryzjerski, a inne globalną korporację, ale - bez względu na wielkość firmy i skalę jej działania - porządek zawsze należy rozpocząć od zlokalizowania wszystkich danych pozostających w obiegu. Następnym krokiem powinno być zdefiniowanie zagrożeń (również tych uwzględniających czynnik ludzki) i przeprojektowanie procesów tak, by je zneutralizować. Zebrane procedury należy też zakomunikować wszystkim pracownikom, a właścicieli danych informować o ich przetwarzaniu.

W ewentualnych rozmowach z UODO kluczowe znaczenie ma bowiem merytoryczne uzasadnienie zastosowania takich, a nie innych procedur i narzędzi. W praktyce, w przypadku małych firm, ważne będzie więc np. legalne i aktualizowane oprogramowanie komputerowe i czytelne oraz zrozumiałe dla każdego pracownika procedury.

W przypadku większych podmiotów, sprawa nieco się komplikuje. Przedstawiciele sektora IT zwracają uwagą na to, że nawet w największych, danymi do niedawno zarządzało się często w najlepszym razie za pośrednictwem excela. „Systemy zgodne z RODO", których wysyp przypadł na drugą połowę 2018 roku, też jednak nie są jednoznaczną odpowiedzią. RODO w żadnym miejscu nie precyzuje, co może oznaczać ten termin. Wybór technologii powinien być rozpatrywany w kategoriach atrybutów, z którymi się wiąże. System, który agreguje dane, które przetwarzamy musi więc być, bezpieczny, integralny i dawać możliwość dostępu do danych w nim zawartych.

ARTYKUŁ PROMOCYJNY

REKRUTACJA A RODO

Anna Bereźnicka
Sales manager, inCV.pl

2

RODO to Ogólne Rozporządzenie o Ochronie Danych Osobowych, które weszło w życie 25 maja 2018 r. Wprowadziło ono takie same zasady ochrony danych osobowych na terenie całej Unii Europejskiej, we wszystkich branżach. Wymagało także zmian w polskim Kodeksie pracy i ustawie o ochronie danych osobowych. RODO nakłada na pracodawców szereg obowiązków związanych m.in. z dostosowaniem prowadzonych procesów rekrutacji do nowych wymagań. Dlatego też systemy HR, z których korzystają firmy, muszą być adekwatne do nowych przepisów.

Głównym zadaniem RODO jest wprowadzenie transparentności w zakresie przetwarzania danych osobowych. Te regulacje są dla pracodawców problematyczne, ale samo wprowadzenie nowych standardów do działów HR firm to jedno. Inną sprawą jest ich utrzymanie na każdym etapie procesu rekrutacji. Tymczasem, zgodnie z wytycznymi organu nadzoru (UODO) w 2019 r. **kontrole dotyczyć będą właśnie obszaru rekrutacji.**

W dokumentach aplikacyjnych, takich jak CV, listy motywacyjne i referencyjne oraz życiorysy, znajduje się sporo informacji o kandydatach. Na ich podstawie dział kadr zbiera dane osobowe potencjalnych pracowników. W świetle prawa jako pracodawca możesz gromadzić jedynie te informacje o aplikantach, które są niezbędne do przeprowadzenia procesu rekrutacji i wyłonienia pracownika o wymaganych kwalifikacjach. W ten sposób stajesz się administratorem ich danych osobowych.

Możesz przeglądać informacje o kandydatach i spośród nich wybierać. Powinieneś jednak zachować przy tym środki ochrony danych osobowych zawarte w RODO. Musisz zapewnić bezpieczny obieg dokumentów aplikacyjnych i chronić je przed osobami postronnymi. CV i listy motywacyjne nie mogą zatem krążyć między pracownikami Twojej firmy, którzy nie biorą udziału w rekrutacji. Muszą

być także odpowiednio przechowywane i usuwane po określonym czasie w skuteczny i trwały sposób (np. poprzez zniszczenie lub odesłanie). Zapewnienie bezpieczeństwa danym dotyczy także najchętniej wybieranej metody pozyskiwania CV od kandydatów, czyli rekrutacji przez Internet.

Twoim obowiązkiem jest zapewnienie najwyższych standardów przetwarzania i ochrony danych. Warto się o to zatroszczyć, bo **kary, jakie może nałożyć UODO za niestosowanie się do rozporządzenia, są poważne.** Sięgają 20 mln euro lub 4 % rocznego światowego obrotu spółki.

Tak dotkliwe sankcje sprawiają, że RODO trzeba traktować poważnie, tym bardziej, że nieznajomość przepisów nie zwalnia z ich przestrzegania. Najwyższy czas zatem przyjrzeć się własnym standardom przetwarzania i ochrony danych w procesie rekrutacji.

Czy masz wdrożone procedury RODO w swoim dziale HR?

- Czy CV, które otrzymujesz od kandydatów, trafiają tylko na określoną skrzynkę e-mail i nie są rozsyłane dalej?
- Czy zawsze kasujesz otrzymane CV w określonym terminie po zamknięciu rekrutacji?
- Czy jeżeli otrzymasz żądanie usunięcia danych kandydata, będziesz w stanie łatwo zlokalizować, czy masz takie CV oraz do kogo mogło trafić?
- Czy wiesz, kiedy dany kandydat wyraził zgodę na przetwarzanie swoich danych?

Jeżeli na którekolwiek z powyższych pytań odpowiedziałeś „nie", to procedury RODO w procesie rekrutacji w Twojej firmie wymagają rewizji.

Dodatkowo zwróć uwagę na to, czy przechowujesz CV kandydatów na dysku wspólnym, do którego dostęp ma więcej niż jedna osoba? A może zdarzyło Ci się przesłać CV kandydata do innej osoby w firmie za pomocą poczty elektronicznej?

Takie działanie stanowi naruszenie przepisów RODO!

Dlaczego procedury RODO w rekrutacji są tak ważne?

Prowadzenie procesu rekrutacji za pośrednictwem systemów wymaga od pracodawcy:

- wykazania podstawy prawnej przetwarzania danych kandydatów,
- zapoznania kandydata z informacją o przetwarzaniu jego danych osobowych,
- zbierania zakresu danych zgodnie z przepisami o ochronie danych osobowych,
- identyfikowania okresów przetwarzania danych w zależności od prowadzonej rekrutacji,
- usuwania danych osobowych zgodnie z określonymi okresami ich przetwarzania,
- usuwania danych osobowych w przypadku cofnięcia zgody na ich przetwarzanie,
- nadawania upoważnień pracownikom mającym dostęp do danych kandydatów,
- eksportu danych kandydatów w celu realizacji prawa do przeniesienia danych.

Wdrożenie i przestrzeganie procedur RODO to zadanie dla wykwalifikowanego zespołu, którego członkowie znają się na prawie i branży IT oraz mają wiedzę i doświadczenie w dziedzinie bezpieczeństwa informacji i przetwarzania danych osobowych...

...tylko gdzie ich znaleźć? Prawda jest taka, że nie musisz szukać ludzi. **Wystarczą odpowiednie narzędzia.** Niektóre portale z ogłoszeniami o pracę oferują systemy zarządzania CV. Niestety, w większości przypadków wymagane jest wówczas korzystanie tylko i wyłącznie z ogłoszeń na jednym, konkretnym portalu. Co więcej, jeśli nawet rekrutujemy kandydatów poprzez wiele różnych portali, to ich dane znajdą się w kilku bazach. To jednak nie jedyny problem. Co zrobić wówczas z aplikacjami kandydatów, które zostały przesłane nie przez portal, lecz trafiły do skrzynki elektronicznej, pocztowej lub zostały przyniesione do sekretariatu firmy? Portale z ogłoszeniami o pracę nie są zatem odpowiednim rozwiązaniem, które sprosta wymaganiom stawianym przez RODO.

W tej sytuacji najpewniejsze będzie korzystanie z jednego systemu, który pozwoli Ci kompleksowo zarządzać i przy tym kontrolować każdy etap rekrutacji.

Rozwiązanie to inCV.pl

Stoimy przed podobnymi wyzwaniami, co Ty, więc przygotowaliśmy skuteczne rozwiązanie w bardzo przystępnej cenie. inCV to narzędzie, dzięki któremu możesz bezpiecznie otrzymywać, przechowywać i zarządzać CV kandydatów na każdym etapie procesu rekrutacyjnego. inCV to gwarancja wdrożenia zgodnych z RODO środków w zakresie ochrony powierzonych Ci danych osobowych.

PROSTE :) I to wszystko punkt po punkcie zgodnie z RODO!

Tyle wystarczy, by przetwarzać dane kandydatów zgodnie z prawem, z czystym sumieniem i bez obawy przed kontrolą UODO.

Co umożliwia inCV.pl?

- prowadzenie procesu rekrutacji zgodnie z obowiązującymi przepisami, a w szczególności z RODO,
- dokumentowanie faktu udzielenia zgody na przetwarzanie danych kandydata oraz zapoznania się z obowiązkiem informacyjnym (co jest wymagane przez RODO), a także:

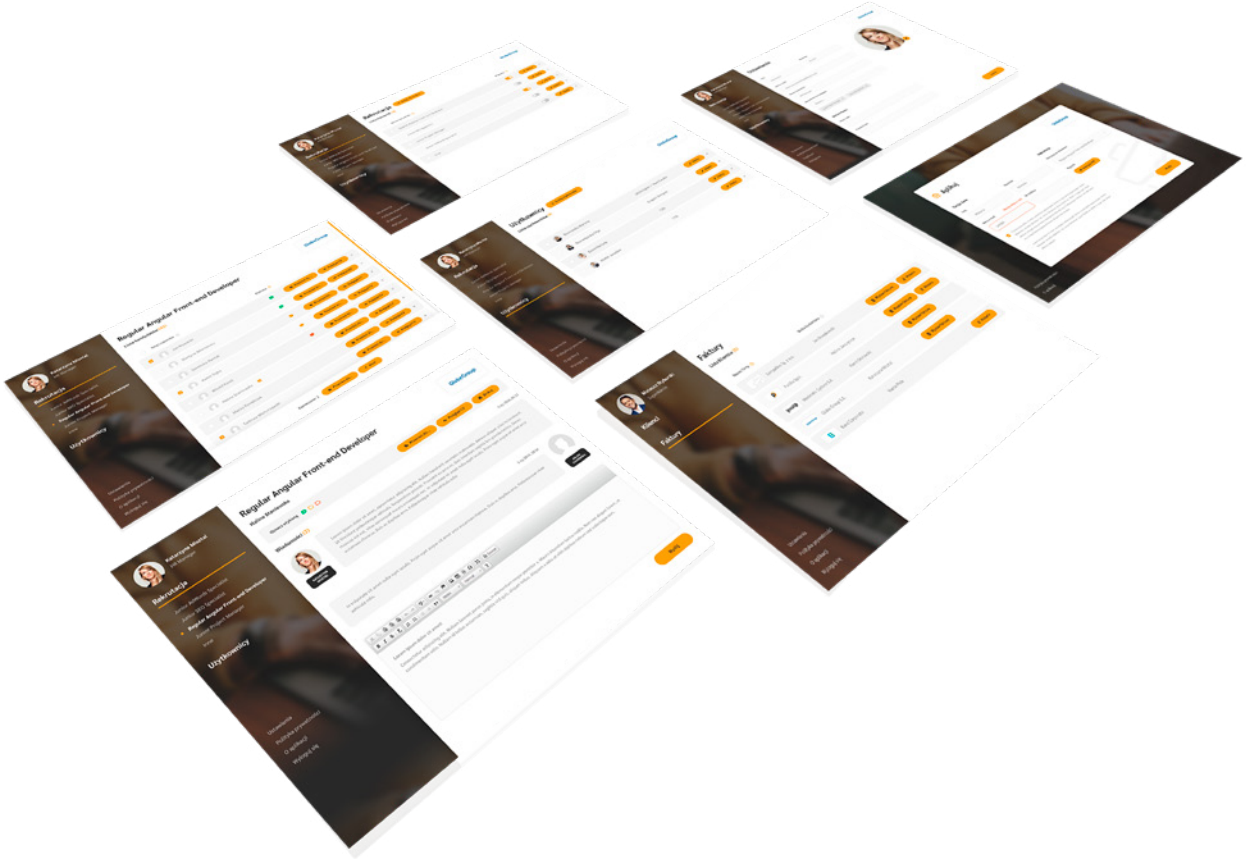
Ile kosztuje inCV.pl?

W inCV.pl przewidzieliśmy **3 podstawowe pakiety** w cenach od 99 zł netto/m-c do 499 zł netto/m-c. Możliwe jest również **rozwiązanie indywidualne**, instalowane na serwerze Twojej firmy oraz integracja z innymi systemami w Twojej firmie.

Zdajemy sobie sprawę, że każde narzędzie najlepiej sprawdzić przed zakupem.

Dlatego dajemy naszym Klientom możliwość **darmowego przetestowania inCV.pl przez okres 30 dni.**

Sprawdź inCV.pl już teraz na www.incv.pl



CYBERATAKI NA FIRMY. SKALA, KONSEKWENCJE, MOŻLIWOŚCI OBRONY

Przemysław Ławrowski
redaktor Interaktywnie.com

pl@interaktywnie.com

3

Już ponad połowa firm narażona jest na cyberataki. Jak pokazują badania, przedsiębiorcy boją się nie tylko pojedynczych hakerów czy zorganizowanych grup zajmujących się cyberprzestępczością, ale także własnych pracowników. Pozytywnym aspektem jest fakt, że większość z nich zdaje sobie sprawę z zagrożenia i w najbliższym czasie planuje inwestycje mające na celu poprawę ochrony IT.

Według opublikowanego w kwietniu 2019 roku raportu KPMG, w 2018 roku 68 procent polskich firm zostało dotkniętych zjawiskiem cyberprzestępczości. Rok wcześniej 82 procent przedsiębiorstw doświadczyło przynajmniej jednego cyberincydentu. Poprawa sytuacji dotyczy również liczbę firm, które w ubiegłym roku odnotowały wzrost liczby cyberataków. Było ich 25 procent - to o 12 pkt. procentowych mniej rok do roku. Z kolei spadek liczby tego typu incydentów zanotowało 8 procent firm, wobec 5 procent w 2017 roku. W oczach przedsiębiorców poprawa jest jednak odbierana jako iluzoryczna, gdyż 7 na 10 firm uważa, że liczba zaobserwowanych prób cyberataków pozostała w 2018 roku na podobnym poziomie, co rok wcześniej.

Liczba cyberataków oraz odsetek firm, których one dotyczyły na przestrzeni 2018 roku

- 0 ataków - 33 procent firm
- od 1 do 3 ataków - 33 procent firm
- od 4 do 9 ataków - 21 procent firm
- od 10 do 29 araków - 8 procent firm
- 30 i więcej ataków - 6 procent firm

Źródło: KPMG

Ile zatem prób cyberataków wykonano? Według ekspertów F-Secure, druga połowa 2018 roku przyniosła ich czterokrotny wzrost, a ich ostateczna liczba wyniosła aż 813 mln. Najczęstszym źródłem pochodzenia ataków są Stany Zjednoczone.

Na drugim miejscu znalazła się Rosja, a na kolejnych Włochy i Wielka Brytania. Trzeba jednak zauważyć, że ataków z USA było prawie 5-krotnie więcej niż z Rosji.

Liczba zarejestrowanych cyberataków w podziale na kraje w drugiej połowie 2018 roku (w mln)

USA	306
Rosja	92
Włochy	58
Wielka Brytania	39
Niemcy	33
Kanada	22
Łotwa	15
Francja	9,3

Źródło: F-Secure

Autorzy cyberataków. Hakerzy czy pracownicy?

Kogo zatem najbardziej obawiają się firmy? Według danych KPMG, około 84 procent przedsiębiorców jako źródło ataku podaje hakerów. Ponad połowa wskazuje również na zorganizowane grupy przestępcze lub cyberterrorystów. Co ciekawe, równie dużo firm upatruje realnego zagrożenia wśród własnych pracowników.

Jak wynika z raportu Cisco, to ludzie korzystający z systemów w firmie są najsłabszym ogniwem w łańcuchu zabezpieczeń.

Z jednej strony zachowania pracowników powodujące potencjalne zagrożenie może wynikać z ich nieświadomych działań. Według badań, najczęściej dotyczą one otwierania załączników nieznanego pochodzenia zawartych w mailach. Złośliwe oprogramowanie w około 1/3 przypadków wysyłane jest poprzez pliki MS Office oraz skompresowane pliki. Na trzecim miejscu znajdują się pliki w formacie pdf.

Największe zagrożenia

Jakich typów ataków najbardziej obawiają się przedsiębiorcy?

- Według danych KPMG, najczęściej wymieniają oni tzw. malware, czyli wyciek danych za pośrednictwem złośliwego oprogramowania.
- Równie często obawiają się oni tzw. ransomware, czyli oprogramowania szpiegującego i szyfrującego dane.
- Jako potencjalne zagrożenie wymieniana jest również kradzież danych przez pracowników oraz zaawansowane kierunkowe ataki APT (z ang. Advanced Persistent Threat).
- Wśród zagrożeń pojawia się również phishing,
- ataki na błędy w aplikacjach
- czy podsłuchiwanie ruchu i ataki Man-in-the-Middle.

Według danych Xopero Software to zaniedbania pracowników są wynikiem aż 48 procent cyberataków. Aby zmniejszyć to ryzyko

niezbędne jest zatem odpowiednie szkolenie załogi z zakresu nie tylko cyberbezpieczeństwa, ale także ochrony wrażliwych danych.

Innym, dużo groźniejszym aspektem, są działania wykonywane rozmyślnie przez pracowników. W takim przypadku szkolenia nie będą oczywiście skuteczne. Pomogą natomiast systemy monitorujące ich aktywność w trakcie pracy.

Jak się ustrzec przed atakiem?

Dobrym rozwiązaniem pomagającym w ochronie danych firmowych jest ich przeniesienie do chmury, czyli skorzystanie z tzw. cloud computingu. Jak pokazują badania przeprowadzone przez Xopero Software, z rozwiązań cloudowych korzysta już 50% firm. To sporo zważywszy na fakt, że tylko 58,3 procent przedsiębiorców uważa to rozwiązanie za bezpieczne. Z kolei według IDC, aż 9 na 10 firm wykorzystuje cloud computing. W swoich przewidywaniach firma idzie jeszcze dalej, gdyż według niej, do 2025 roku biznes przeniesie 60 procent danych do chmury. Widać zatem, że zalety tego rozwiązania przewyższają strach, jaki ono budzi. Cloud computing to nie tylko wygoda i niski koszt utrzymania i wdrożenia, ale także - wbrew obiegowej opinii - bezpieczeństwo.

Dlaczego firmy nie ufają rozwiązaniom chmurowym

Mam wrażenie, że te statystyki o nieufności przedsiębiorców do chmury mają swoje podłoże w dwóch źródłach. Pierwszym jest dość abstrakcyjny i nienamacalny charakter rozwiązań cloudowych. Drugą przyczyną są powszechne mity na temat chmury. Obawy o to, że jest ona niebezpieczna, droga czy mało wydajna są bezpodstawne. Dostawcy usług chmurowych korzystają z takiego poziomu zabezpieczeń, którego wdrożenie w pojedynczym przedsiębiorstwie jest co najmniej nieopłacalne, a często wręcz niemożliwe

Bartosz Jurga
Head of Sales w Xopero Software

Chmura"oferuje również rozwiązania SECaaS (z ang. Security-as-a-Service). Zabezpieczenia te szybko ewoluują wraz z nowymi zagrożeniami. Według szacunków, globalna wartość tego rynku wyniesie w 2020 roku około 8,5 mld dolarów. Firmom nie opłaca się zatem budować strzeżonej serwerowni i wolą oddać dane w ręce specjalistów.

Inwestycje na bezpieczeństwo

Zdaniem ekspertów z Xopero Software, prawie połowa przedsiębiorców deklaruje chęć zwiększenia wydatków na bezpieczeństwo IT. Jak wynika z informacji przesłanej do Interaktywnie.com, największe inwestycje firmy planują w obszarze backupu i rozwiązań disaster recovery, czyli zapasowych centrów danych, które w razie awarii są w stanie w krótkim czasie przejąć najważniejsze funkcjonalności. Według danych, chęć wdrożenia właśnie takich zabezpieczeń deklaruje

niemal 65 procent firm. Przy tym 48 procent z nich zamierza zwiększyć nakłady także na antywirusy, oprogramowania antyspyware lub firewall. Z kolei z danych PWC wynika, że w polskich przedsiębiorstwach do tej pory najczęściej wykorzystywanym zabezpieczeniem (53 procent) były firewalle aplikacyjne (WAF) oraz systemy detekcji włamań (IPS/IDS), na które zdecydowało się 52 procent firm.

Odsetek firm deklarujących przynajmniej dostateczną dojrzałość obszarów zabezpieczeń

- Co najwyżej w połowie analizowanych przypadków (88 procent)
- W większości analizowanych przypadków (12 procent)
- W każdym z analizowanych przypadków (0 procent)

Źródło. KPMG

Dane KPMG pokazują, że firmy w najbliższym czasie planują wdrożyć lub zwrócić większą uwagę na kilka kluczowych działań mających wpływ na bezpieczeństwo ich systemów informatycznych oraz danych. Wśród nich są plany zapewnienia ciągłości działania, wprowadzenia zabezpieczeń na styku z siecią, reagowanie na incydenty, bezpieczeństwo sieci wewnętrznej (kontrola dostępu, segmentacja), a także monitorowanie bezpieczeństwa.

Jak się okazuje, obecnie niewiele firm jest w pełni zadowolona z wprowadzonych przez siebie zabezpieczeń. W większości analizowanych obszarów ochronę pozytywnie ocenia 12 procent przedsiębiorstw, a 88 procent dobrze ocenia co najwyżej połowę z nich. Dojrzałość swojego systemu bezpieczeństwa na poziomie pełnym najwięcej firm określiło w przypadku ochrony przed złośliwym oprogramowaniem. Najsłabiej natomiast ocenili oni natomiast swoje zabezpieczenia dotyczące urządzeń mobilnych.

Eksperci potrzebni od zaraz

Jak wskazuje 63 procent firm, największym problemem, który wiąże się z budową stabilnego systemu bezpieczeństwa w firmie jest brak wykwalifikowanych pracowników. Według danych Cisco, w polskich firmach pracuje obecnie tylko około 5 tys. specjalistów z tej dziedziny. Przedsiębiorstwa zatrudniające nie więcej niż 300 osób często decydują się zatrudnić osobę odpowiedzialną za cyberbezpieczeństwo. Więksi gracze natomiast tworzą w tym celu dedykowany 2-3 osobowy zespół. Mała podaż ekspertów specjalizujących się w tej dziedzinie sprawia, że do rzadkości nie należą zarobki na poziomie 15 tys. zł brutto lub więcej. Przydatnymi w pracy na tych stanowiskach są certyfikaty takie jak CISSP, CISA, CISM, CRISC i Lead Auditor ISO 27001, które potwierdzają odpowiednie umiejętności. W grę wchodzą również certyfikaty hakerskie takie jak, CEH, GSEC, OSCP.

Problemem może być budżet

Mimo że rozwiązania z zakresu cloud computingu są znacznie tańsze, to i tak sporo firm boryka się z niedostatecznym budżetem przeznaczonym na poprawę cyberbezpieczeństwa. Z danych KPMG wynika, że ten problem sygnalizuje 61 procent firm.

Jak pisała firma Michael Page w swojej informacji prasowej opublikowanej na łamach Interaktywnie.com, "należy zaznaczyć, że firmy będąc coraz bardziej świadome zagrożeń cybernetycznych, coraz chętniej alokują dodatkowe środki na ten obszar. Potwierdzają to m.in. dane zebrane przez analityków IDC, z których wynika, że wydatki na odpowiednie rozwiązania - w tym sprzęt i oprogramowanie oraz usługi - wyniosą w 2019 roku 27,3 mld dolarów. Stanowi to więc wzrost o 8,3 procent w stosunku do ubiegłego roku".

Dane IDC pokazują również, że w 2019 roku ponad połowa wydatków w Europie związanych z bezpieczeństwem IT będzie dotyczyć usług. Firmy wydadzą w ten sposób 14,8 mld dolarów. Składać się na to będą tzw. zarządzanie usługami bezpieczeństwa i usługi integracyjne. Oprócz tego 8,6 mld dolarów obejmą wydatki związane z oprogramowaniem, a 3,9 mld dolarów ze sprzętem.

10 trendów związanych z cyberbezpieczeństem

Firmy technologiczne inwestują coraz większe zasoby w migrację do kultury zwinnego wytwarzania oprogramowania, co niesie ze sobą konieczność implementacji zautomatyzowanych mechanizmów dla zapewniania jakości oraz bezpieczeństwa produktów i infrastruktury.

Korporacje wydzielają znaczną część budżetów na edukację pracowniczą w zakresie cyberzagrożeń, skupiając się na zagadnieniach związanych z inżynierią społeczną oraz atakami phishingowymi. Można spodziewać się zwiększonych nakładów na implementację kultury DevSecOps, zgodnie z którą każdy pracownik jest współodpowiedzialny za bezpieczeństwo organizacji.

Ataki ransomware nie znikną, gdyż są zbyt dochodowe. Można jednak spodziewać się przeniesienia wektora ataku na korporacyjne infrastruktury serwerowe, aniżeli na komputery prywatne użytkowników. Firmy będą gotowe zapłacić o wiele więcej za odzyskanie dostępu do infrastruktury, na której opiera się funkcjonowanie ich biznesu.

Biorąc pod uwagę ogromną skalę wycieków danych w 2018 roku, w tym roku firmy oczekują o wiele wyższego

bezpieczeństwa od swoich dostawców oprogramowania. Coraz szybciej zmierza się w kierunku, w którym firmy będące liderami bezpieczeństwa będą zagarniać większą część rynku korporacyjnego, któremu zależy na stabilnej usłudze oraz poufności danych klientów.

W roku 2018 widzieliśmy kilka drobnych pozwów wynikających z ustawy RODO, ale to w 2019 zobaczymy prawdziwie kosztowne sprawy sądowe skierowane w firmy, które nieodpowiednio zadbały o procesy bezpieczeństwa w swoich organizacjach i pozwoliły na wycieki wrażliwych danych użytkowników.

Organizacje rządowe rozpoczynają prace nad analizą wpływu cyfrowych technologii uzależniających na bezpieczeństwo narodowe oraz przygotowanie planów mających na celu zmniejszenie ich negatywnego oddziaływania na zdrowie społeczeństwa, gospodarkę oraz stan cyberbezpieczeństwa kraju.

Kampanie dezinformacyjne nabierają jeszcze większego rozpędu, szczególnie ze względu na rozwój technologii sztucznej inteligencji, która w coraz bardziej wiarygodny sposób pozwala preparować wypowiedzi polityków i innych kluczowych osób.

Ataki phishingowe stają się bardziej zaawansowane i coraz częściej wykorzystują zaufane platformy służące do dzielenia się plikami, jak np. Google Drive.

Rozwinięcie sieci 5G oznacza jeszcze więcej urządzeń podłączonych do Internetu Rzeczy. Lodówki, samochody, kamery dla dzieci, konsole, telewizory i wiele innych urządzeń pozwala cyberprzestępcom na zdalne uzyskiwanie dostępu do prywatnych rejonów życia.

Biorąc pod uwagę podejście nowych pokoleń do prywatności w sieci, śmiałego dzielenia się poufnymi informacjami na portalach społecznościowych oraz nierzadkie przypadki wycieków danych, można spodziewać się wielu dyskusji na tym tle. Jest to temat bardzo zaawansowany społecznie, jednak zdecydowanie każdy dyrektor odpowiedzialny za bezpieczeństwo danych powinien pozostawać na bieżąco z formującymi się normami społecznymi odnośnie prywatności w sieci.

Dawid Bałut
ekspert w zakresie cyberbezpieczeństwa z TestArmy CyberForces

Źródło: https://interaktywnie.com/biznes/newsy/bezpieczenstwo/cyberbezpieczenstwo-10-trendow-ktore-zdominuja-kierunek-rozwoju-tego-sektora-258519

Możliwe skutki biznesowe zagrożenia dla przedsiębiorców

To, co może się stać w przypadku zbyt luźnego podejścia do tematów związanych z cyberbezpieczeństwem pokazują przykłady. Dane dotyczące swoich pacjentów niedawno mogła utracić firma świadcząca usług medyczne z Massachusetts w USA. Atak przeprowadzono za pomocą oprogramowania szantażującego GandCrab.

- W ostatnich latach hakerzy szczególnie gustują w atakach na instytucje opieki zdrowotnej i ich zaplecze. Infekują systemy IT oprogramowaniem szantażującym (ransomware) lub wstrzykują złośliwy kod, mający za zadanie kradzież danych, które następnie wykorzystywane są w przyszłych oszustwach - komentuje w informacji prasowej Jakub Tarczyński, inżynier techniczny Bitdefender z firmy Marken.

Co ciekawe, fakt przeprowadzenia ataku wykryto dopiero półtora roku po jego faktycznym dokonaniu. Firma odmówiła zapłaty okupu, a więc nie można wykluczyć, że hakerzy mogą chcieć wykorzystać nielegalnie zdobyte dane. Mogli oni wykraść takie informacje jak imiona i nazwiska pacjentów, a także ich adresy, daty urodzenia, numery ubezpieczenia społecznego, numery prawa jazdy czy nawet dane dotyczące ich stanu zdrowia.

Z kolei w inny haker włamał się do ambasady Meksyku w Gwatemali i wykradł prawie 5 tysięcy poufnych dokumentów. Zginęły dane osobowe dyplomatów i obywateli Meksyku, w tym kserokopie paszportów, aktów urodzenia, wiz i kart płatniczych oraz informacje dotyczące immunitetów, przywilejów, kosztów medycznych. Haker wykrył lukę w zabezpieczeniach serwera obsługującego te dokumenty, o czym początkowo poinformował urzędników. Brak odzewu dotknął go jednak osobiście, co było punktem zapalnym do dokonania cyberataku. Jak widać nie tylko zaniedbania w kwestii bezpieczeństwa IT mogą mieć złe skutki. W tym przypadku zlekceważenie hakera okazało się jeszcze gorsze w skutkach.

Zgodnie z analizą firmy Mimecast - zarządzającej wiadomościami Microsoft Exchange oraz Microsoft Office 365 - liczba ataków phishingowych dynamicznie wzrasta. Od sierpnia 2018 do lutego 2019 zwiększyła się aż o 126% (!) Sporo, jak na tak krótki przedział czasu.

W ramach badania przeanalizowano łącznie 28 407 664 wiadomości mailowych dostarczonych do korporacyjnych skrzynek pocztowych. Nadmienić należy, że wiadomości te "prześwietlone" zostały uprzednio przez firmowe systemy bezpieczeństwa i sklasyfikowane jako niegroźne. Czy faktycznie takie były? Niestety, w 463 546 spośród nich odnaleziono złośliwe adresy URL. Oznacza to, że średnio co 61. mail lądujący w firmowej skrzynce odbiorczej może stanowić zagrożenie dla bezpieczeństwa firmy.

ARTYKUŁ PROMOCYJNY

JAK CHRONIĆ SIĘ PRZED ATAKAMI? SOFTWARE I HARDWARE POMOGĄ UNIKNĄĆ ZAGROŻEŃ.

Marcin Sztanderski
Dyrektor ds. Wdrożeń w Cloudware Polska

4

W dobie rosnących zagrożeń w sieci, coraz ważniejsze staje się dbanie o kwestie związane z bezpieczeństwem. Dotyczy to zarówno małych, średnich, jak i dużych przedsiębiorstw. O tym, jak chronić się przed atakami, w jakie rozwiązania inwestować oraz co obecnie grozi organizacjom, opowiada Dyrektor ds. Wdrożeń w Cloudware Polska, Marcin Sztanderski.

Czy możemy mówić o natężeniu ilości cyberataków w ostatnich latach?

Poziom zagrożenia w zakresie wszelkiego rodzaju ataków stale rośnie, przede wszystkim z uwagi na fakt, że istnieje coraz więcej metod i źródeł zagrożenia. Systemy są coraz bardziej skomplikowane, zachodzi między nimi coraz większa ilość interakcji, przez co przepływ danych jest także coraz szybszy. Przez to użytkownicy mają mniej czasu na analizę tego, co się faktycznie dzieje. Świetnym przykładem jest zyskująca coraz większą popularność koncepcja powszechnego wykorzystania API. Systemy można bardzo łatwo zintegrować, ale trudno jest zapanować nad tym kto, kiedy i do czego ma dostęp, przez co organizacje częściowo utraciły - lub tracą - kontrolę nad przepływem informacji.

Jak w takim przypadku radzić sobie z tego typu zagrożeniami?

Remedium na tego typu wyzwania może być system IBM Guardium, który nadzoruje i zabezpiecza dostęp do danych zgromadzonych w repozytoriach różnych typów np. relacyjne bazy danych, pliki płaskie, dane nieustrukturowane. Co istotne, system zapewnia bezpieczeństwo na poziomie aplikacji, ale też operatorów pracujących bezpośrednio przy

repozytoriach danych. Jest to świetne narzędzie dla wszystkich organizacji, które gromadzą duże ilości danych, w tym dane osobowe. A jak doskonale wiemy, nowe przepisy RODO są bardzo rygorystyczne również w zakresie zabezpieczania danych przez organizacje.

Obszar Security jest bardzo rozległy, w związku z tym nasuwa się pytanie: czy oprócz samych danych, firmy powinny zwrócić uwagę na inne aspekty?

Tak, kluczowym – i niestety najczęściej najsłabszym – ogniwem są ludzie. W związku z tym istotne jest, aby dostęp pracowników do danych przedsiębiorstwa, w tym danych osobowych, funkcji oraz procesów odbywał się w sposób kontrolowany i podlegający weryfikacji. W tej sytuacji z pomocą przychodzą nam rozwiązania z rodziny zarządzania tożsamością (Identity Management), które z jednej strony wspomagają działy HR i Marketingu w sprawnym wykonywaniu procesów związanych z zarządzaniem personelem, jak i np. danymi klientów, automatyzując zadania związane z on i off boardingiem pracowników oraz przypisywaniem ról w aplikacjach i systemach. Ważną cechą tego typu rozwiązań jest też możliwość centralnego zarządzania uprawnieniami. Dotyczy to zarówno administratorów IT, jak i pracowników pozostałych departamentów w ramach danej organizacji.

Kolejną wartością dodaną jest możliwość uruchomienia pojedynczego logowania. W praktyce oznacza to, że raz uwierzytelniona osoba ma dostęp tylko do wskazanych systemów, zgodnie z polityką przedsiębiorstwa. Dzięki temu pracownicy nie muszą przechowywać i znać wielu haseł, co zmniejsza ryzyko wejścia w ich posiadanie osób postronnych. Warto także przypomnieć, że oprócz typowych narzędzi IT, istotnym elementem jest budowanie odpowiedniej świadomości wśród pracowników. Przykładem może być tutaj pilnowanie dostępu do haseł i PINów, tak by nie trafiły one w ręce nikogo spoza organizacji. Blokowanie dostępu do komputera przy każdym odejściu od biurka jest równie ważne, gdyż nigdy nie wiemy, kto dokładnie znajduje się na terenie organizacji.

Jak ze wskazanymi zagrożeniami mogą radzić sobie działy IT?

Pozytywnym trendem, który można zaobserwować, jest powoływanie dedykowanych zespołów zajmujących się tylko bezpieczeństwem informatycznym w ramach danej organizacji. Oznacza to, że już nawet małe i średnie przedsiębiorstwa rozumieją, jak ważna jest kwestia zabezpieczenia dostępów do systemów informatycznych, gdyż to na nich oparte są najcenniejsze zasoby przedsiębiorstwa takie jak: dane osobowe, wiedza, procesy czy kontrola produkcji. W tym przypadku kluczowa jest

kompleksowa wiedza o tym, co dzieje się w organizacji od strony IT. Wiodącym rozwiązaniem w tej kategorii jest system QRadar, który zbiera, agreguje i koreluje zdarzenia z wielu warstw środowiska informatycznego. Dzięki temu specjaliści ds. bezpieczeństwa uzyskują natychmiastową i kompleksową informację na temat zdarzeń mogących zagrozić bezpieczeństwu informatycznemu przedsiębiorstwa. Na tej podstawie mogą szybko zareagować i zminimalizować koszty utraty danych lub wstrzymania produkcji.

Jeśli dział bezpieczeństwa posiada już wiedzę na temat zdarzeń zachodzących w środowisku IT, co może zrobić, by w jak najskuteczniejszy sposób reagować na te zagrożenia?

Odnosząc się do początku rozmowy, warto ponownie zwrócić uwagę, że środowiska informatyczne są coraz bardziej skomplikowane i rozproszone. Dotyczy to także usług chmurowych. W związku z tym wiedza ekspertów musi być coraz bardziej rozległa. Rodzi to problemy zarówno ze strony kadry, jak i kosztów utrzymania. Dlatego w tym przypadku ważne jest wykorzystanie oprogramowania, które wspiera organizacje w szybkim i efektywnym rozwiązaniu incydentów bezpieczeństwa. Aplikacja IBM Resillient wspiera operatorów działu bezpieczeństwa poprzez korelacje danych z systemów wewnętrznych i zewnętrznych repozytoriów danych oraz dodatkowo podpowiada schematy rozwiązywania i niwelowania zagrożeń. Dzięki temu utrzymaniem odpowiedniego poziomu bezpieczeństwa mogą zajmować się osoby nie tylko z kompetencjami na poziomie eksperckim.

Obecnie firmy pracują w coraz bardziej zglobalizowanej gospodarce, co wiąże się z koniecznością ciągłej wymiany informacji z wieloma partnerami. Jak w takim przypadku przedsiębiorstwo może zadbać o bezpieczeństwo?

Wielokierunkowy przepływ danych jest obecnie niezbędny i wręcz oczywisty w dobie gospodarki 2.0. W związku z tym niezwykle istotne jest, aby ten przepływ był wydajny i bezpieczny. W tym aspekcie świetnym rozwiązaniem jest technologia blockchain. Dzięki zastosowaniu algorytmów kryptograficznych gwarantuje ona spójność i niezmienność danych, a dzięki rozproszonej infrastrukturze przechowywania jest odporna na awarie i zakłócenia w działaniu sieci.

W czym zatem tkwi atrakcyjność blockchaina?

Potencjał blockchaina jest trudny do przecenienia i nie należy wiązać go wyłącznie z kryptowalutami. Technologia łańcucha bloków stawia na przejrzystość i pełny brak anonimowości,

w związku z czym może być wykorzystywana w biznesie, usprawniając tym samym wiele procesów w ramach danej organizacji. Technologia ta jest prosta do implementacji i nie wymaga inwestowania dodatkowych, dużych kosztów w zaplecze techniczne po stronie Klienta. Co więcej, jest to w pełni przejrzyste od strony technologicznej rozwiązanie, sprawdzone w zastosowaniach biznesowych zarówno w Polsce, jak i na świecie. Coraz większe instytucje sięgają po blockchaina, chociażby w zakresie działań związanych z obiegiem dokumentów, logistyką czy nawet weryfikacją autentyczności swoich produktów. Sama technologia została stworzona z myślą o bezpieczeństwie i niezmienności danych, co jak wiadomo jest obecnie jednym z kluczowych wyzwań, nie tylko dla branży IT.

POZYSKIWANIE, PRZETWARZANIE I WYKORZYSTYWANIE DANYCH KLIENTÓW ORAZ PARTNERÓW. JAK ROBIĆ TO ZGODNIE Z PRAWEM

Paweł Musiał
redaktor Interaktywnie.com

pm@interaktywnie.com

5

Jak prowadzić kampanie w zgodzie z przepisami. Czy można kupować bazy adresowe. Jak zabezpieczyć już posiadane. Jak stosować e-mail marketing zgodnie z prawem. Jak prowadzić zapisy na newsletter. Jakich danych zbierać nie wolno. Jak zmienią się zasady telemarketingu. Do kogo mogą dzwonić telemarketerzy. Jak umawiać spotkania biznesowe zgodnie z prawem. Jak należy chronić bazę z numerami telefonów. Takie pytanie powinien zdać sobie każdy pracownik marketingu. Czy każdy to robi?

Informowanie to praktyka, która musi wejść w krew wszystkim marketerom. Poza własnymi danymi kontaktowymi przedsiębiorca wciąż musi informować o podstawie prawnej, która pozwala mu zbierać informacje. To jednak nie wszystko. Konsumenci muszą być świadomi tego, przez jaki czas, w jaki sposób oraz w jakim celu i zakresie firma przetwarza i wykorzystuje ich dane osobowe. Jeśli przedsiębiorca zamierza przekazać te dane innemu podmiotowi, również musi to jasno zakomunikować i uzyskać odrębną zgodę.

Powierzający swoje dane muszą też zostać poinformowani o przysługujących im prawach. Mieć świadomość, że zawsze mogą zażądać wglądu do tego, jakie dane są wykorzystywane w handlu internetowym, posiadać możliwość ich przeniesienia, zmiany (tzw. prawo do sprostowania), a nawet całkowitego ich usunięcia (słynne prawo do bycia zapomnianym).

W każdej chwili również mają prawo wycofać się ze zgody na przetwarzanie tych informacji lub zmiany ich zakresu. Na dodatek, w razie, gdyby klient uznał, że jego dane są niewłaściwie wykorzystywane, albo prawa nie są respektowane - ma możliwość wniesienia skargi do organu nadzorującego.

RODO wymusza minimalizację

Zbierać można tylko te dane, które są nam faktycznie potrzebne. Przy ewentualnej kontroli można się spodziewać pytania

o to, do czego dana informacja przedsiębiorcy jest potrzebna. Wówczas trzeba mieć sensowny argument potwierdzający zasadność pozyskiwania takiej informacji o kliencie.

Dobrym przykładem będzie zbieranie daty urodzin klienta przy składaniu zamówienia w e-sklepie. Ciężko uzasadnić zbieranie tego typu informacji do celów jego realizacji. A cele marketingowe to inna kwestia. W myśl przepisów RODO powinny być w tym momencie rozdzielone. Rozporządzenie wymaga bowiem dodatkowej zgody na przesyłanie ofert handlowych, a osobnej na zapis do newslettera.

Użytkownik musi też zostać poinformowany o profilowaniu jego danych i wyrazić na nią świadomą zgodę - albo jej odmówić.

Ważne jest jednak to, że zgody wymaga jedynie profilowanie danych, które umożliwiają identyfikację. Zgodnie z RODO wykorzystywanie narzędzi, które bazują na profilowaniu zachowania anonimowych użytkowników - jak choćby popularny Google Analytics - to ono nie obowiązuje.

Bezpieczeństwo i zabezpieczenia

RODO wprowadziło tzw. procedurę autodenuncjacji. Przedsiębiorca ma obowiązek poinformować w ciągu 72 godzin o wycieku i podjętych krokach zapobiegawczych organ nadzorujący, a w razie wysokiego ryzyka naruszenia praw lub wolności osób fizycznych, także osobę, której dane dotyczą.

Choć RODO nie zwalnia przedsiębiorcy z odpowiedzialności, to może mieć znacznie przy ustalaniu zakresu odpowiedzialności. Nowe przepisy dają swobodę w kształtowaniu zabezpieczeń przez firmę, które jednak powinny być adekwatne do zagrożeń. Należy pamiętać, że po stronie firmy jest obowiązek dowodowy. Kontrolerzy badając zgodność z przepisami RODO, będą pytać, jak zabezpieczane są dane i dlaczego stosowane są takie, a nie inne zabezpieczenia w kontekście ryzyka, jakie mogą wystąpić. Zawsze można się także próbować powoływać na brak winy w wyborze.

Dobuble opti-in czyli zasada permission marketingu

Subskrybent jakiejkolwiek usługi w internecie musi wyrazić zgodę na działania marketingowe dobrowolnie, świadomie i w sposób bezpośredni, tak by nie było żadnych wątpliwości, że dana osoba, chce i zgadza się udostępnić swoje dane, otrzymywać newsletter i oferty handlowe.

Mechanizmem, który będzie zgodny z rozporządzeniem i da firmie pewność, że zgoda została wydana świadomie i dobrowolnie, może być tzw. model podwójnych maili potwierdzających - dobuble opti-in.

To proces, który wymaga potwierdzenia chęci otrzymywania wiadomości przez daną osobę, zanim zostanie dodana ona do listy odbiorców. Takie potwierdzenie może odbywać się poprzez kliknięcie w link, który zostaje wysłany do odbiorcy w wiadomości. Jego brak automatycznie oznacza, że tej zgody nie ma. Tym sposobem firma ma jasność i pewność, że nie łamie postanowień RODO.

Prosta rezygnacja

W ramach pozyskiwania zgód w kampaniach e-mail marketingowych konieczne jest umożliwienie klientowi rezygnacji i wycofania się z udostępnienia wszelkich pozwoleń na przetwarzanie i wykorzystywanie danych osobowych.

Trzeba jednak pamiętać, że musi być to równie łatwe, co ich zatwierdzenie. To znaczy, że specjalny przycisk dezaktywujący np. newsletter powinien być umieszczony w każdym mailingu. Klient nie powinien musieć go szukać. Jego rozmiar, kolor czy grafika powinna być nieodbiegająca od linków aktywujących.

RODO wymaga też, aby komunikować się z klientami w sposób prosty i zrozumiały, co oznacza zmiany również we wszelkich formularzach.

Najważniejsze zasady RODO

- Firmy przetwarzające dane osobowe muszą bezdyskusyjnie umożliwić klientowi korzystanie z szeregu praw, które wprowadza RODO. Mowa między innymi o prawie do bycia zapomnianym (a więc wykreślenia wszelkich danych z bazy na żądanie), prawie do zmiany informacji albo ich przeniesienia do innego administratora danych (na dodatek na ujednoliconym nośniku, tak aby nie pojawiła się trudność z ich odczytaniem w nowym miejscu);

- utrudnione jest profilowanie, czyli zautomatyzowane przetwarzanie danych osobowych, kończące się niekiedy tym, że niektórzy konsumenci mogli zostać wykreśleni z grupy osób, którym należy się kredyt, bowiem „z automatu" zadecydowały o tym pewne ich cechy;

- wprowadzona zostaje zasada minimalizacji przetwarzanych danych, a to oznacza, że firmy powinny gromadzić i posługiwać się tylko niezbędnym do funkcjonowania minimum tego rodzaju informacji. W związku z tym RODO rozprawia się również ze spamem i niechcianymi zapytaniami ofertowymi, składanymi na przykład przez telemarketerów;

- zmienia się kształt umów o powierzeniu i podpowierzeniu danych, a więc dotyczących sytuacji, kiedy administrator danych osobowych korzysta z pomocy innej firmy i udostępnia jej tego rodzaju informacje. Umowy są więc dokładniejsze, bardziej rozbudowane, a niepoprawne ich przygotowanie skutkuje nawet otrzymaniem bardzo wysokich kar;

- wprowadzone zostają dwie zupełnie nowe zasady – privacy by design i privacy by default, które mają ogromny wpływ na to, jak przetwarzane będą dane osobowe w firmach. Po pierwsze, odtąd już na etapie kreowania nowych systemów lub technologii, trzeba mieć na uwadze wymaganą przez RODO ochronę danych. Myślenie o bezpieczeństwie tego rodzaju informacji jest wpisane w prace nad każdym projektem, który wiąże się z przetwarzaniem danych osobowych. Po drugie, w automatycznych ustawieniach konieczne jest ustawienie ochrony danych. Zmiana wymaga aktywnej i świadomej działalności osoby, której te informacje dotyczą;

- firmy są zachęcane do tego, by korzystać z takich rozwiązań ułatwiających ochronę danych osobowych, jak: personalizacja, pseudonimizacja albo szyfrowanie;

- zapytania o zgody na przetwarzanie danych osobowych muszą przestrzegać szeregu reguł – na przykład być napisane, inaczej, niż dotąd, przystępnym językiem, zrozumiałym dla odbiorcy i wyjaśniającym sposób oraz cel tego przetwarzania;

- niektóre z firm muszą przeprowadzić ocenę skutków dla ochrony danych osobowych aby udowodnić, że jak najlepiej przygotowały firmę do wejścia w życie rozporządzenia;

- w przypadku naruszenia bezpieczeństwa danych osobowych firmy mają obowiązek reagować w czasie do 72 godzin po wydarzeniu, w przeciwnym razie grożą im poważne kłopoty. A jak powinny reagować? RODO dokładnie opisuje procedurę oraz konstrukcję zgłoszenia, przekazywanego GIODO;

- zmienia się również podejście do samych zbiorów danych osobowych. Dotąd należało je zarejestrować w GIODO. Zamiast tego trzeba jednak prowadzić rejestr czynności przetwarzania danych;

- zamiast dotychczasowego administratora bezpieczeństwa informacji, którego obecność była dobrowolna, pojawia

- się inspektor ochrony danych. W niektórych, ściśle określonych firmach, jego wyznaczenie jest obowiązkowe, w przeciwnym razie znów – grożą bardzo wysokie kary;

- • RODO podtrzymuje konieczność upoważniania wybranych pracowników do przetwarzania danych osobowych, opartego między innymi na zobowiązaniu do zachowania tajemnicy i należytej ochronie tego rodzaju informacji;

- • przepisy wprowadzone przez RODO obejmują również firmy spoza Unii Europejskiej, jeśli przetwarzają one dane osobowe ludzi przebywających na terenie Wspólnoty oraz ich wykorzystanie jest związane z monitorowaniem zachowania tych osób oraz z oferowaniem im różnego rodzaju usług lub towarów.

Privacy by design i privacy by default

Po wejściu w życie RODO nie wystarczy wprowadzenie odpowiedniego rozwiązania zmierzającego do ochrony danych osobowych w istniejących już technologiach. Trzeba będzie mieć je na uwadze już na etapie tworzenia nowych. A to nie wszystko, co powinieneś wiedzieć na temat nowych zasad wprowadzonych przez RODO.

Wraz z nowym rozporządzeniem, w polskim systemie prawnym pojawią się dwie, zupełnie nowe zasady, związane z ochroną danych osobowych privacy by design oraz wynikająca z niej privacy by default.

W rozporządzeniu czytamy:

„uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikające z przetwarzania, administrator – zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania – wdraża odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi niniejszego rozporządzenia oraz chronić prawa osób, których dane dotyczą".

Oznacza to, że odtąd na każdym etapie projektowania nowego systemu albo technologii, służących do przetwarzania danych osobowych, zasady ochrony tych informacji będą musiały być respektowane. Innymi słowy, privacy by design (inaczej: zasada prywatności w fazie projektowania) wymaga, aby zawsze istniały narzędzia służące do odpowiedniego przetwarzania danych osobowych oraz do ich ochrony.

Privacy by default, zwana również zasadą prywatności w ustawieniach domyślnych wymaga, aby każdy system w domyślnych ustawieniach miał przypisaną ochronę danych osobowych. Rozporządzenie posiada bowiem następujący zapis:

„Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania. Obowiązek ten odnosi się do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności."

Wynika z tego, że z automatu można będzie pozyskiwać jedynie całkowite minimum informacji, dotyczących użytkownika. Aby się to zmieniło, potrzebne będzie działanie jego samego.

Z powyższymi zasadami ściśle wiąże się mechanizm Privacyimpactassessment, również wprowadzony przez RODO. Opisuje on kolejny, bardzo ważny obowiązek administratora: „jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych".

Jak wynika z rozporządzenia, wywiązywanie się z powyższych obowiązków będzie można wykazać między innymi poprzez wprowadzenie zatwierdzonego mechanizmu certyfikacji. Sama certyfikacja ma być dobrowolna i nie wpływać na obowiązki administratora, wynikające z RODO. Dokonywać jej będzie wyznaczony w danym europejskim kraju podmiot certyfikujący albo organ nadzorczy. Udzielana ma być na trzy lata, jednak możliwe będzie jej przedłużenie.

Czas na inspektorów ochrony danych

Do tej pory w Polsce działali administratorzy bezpieczeństwa informacji (ABI), jednak z wejściem w życie RODO w ich miejsce wprowadzeni zostaną inspektorzy ochrony danych (IOD). Funkcje podobne, jednak o ile obecność w firmie ABI nie była obowiązkowa, o tyle nowego inspektora w niektórych przypadkach już owszem. I znów przestroga – przedsiębiorstwo, które obowiązku nie dopełni, będzie się musiało liczyć z karami.

Rozporządzenie w artykule 37. wskazuje trzy grupy administratorów i podmiotów przetwarzających dane osobowe, którzy będą do tego zobowiązani.

W pierwszej mowa o organach lub podmiotach publicznych, *"z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości". W drugiej o firmach, w których „główna działalność administratora lub podmiotu przetwarzającego polega na operacjach*

przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę".

Jest też trzecia grupa. To firmy, w których „główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych, takich jak ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzające dane genetyczne, dane biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej tej osoby, jak również dane osobowe dotyczące wyroków skazujących i naruszeń prawa".

Co to dokładnie oznacza? Przepisów wykonawczych jak dotąd brak. Głowią się więc nad tym zagadnienie kancelarie prawne wielu korporacji.

Co ciekawe, IOD nie będzie najprawdopodobniej ponosił żadnych odpowiedzialności, bo za przetwarzanie danych, odpowiada ich administrator, ewentualnie podmiot, któremu administrator powierzył te dane. W małych i średnich firmach faktycznie odpowiedzialność skoncentruje się więc na zarządzie.

Formularze internetowe zgodne z RODO

Zapytaliśmy u źródła, czyli w Urzędzie Ochrony Danych Osobowych, jak powinny one wyglądać.

Właściciel lub administratorzy strony i portali internetowych (w tym także firmowych) powinni pamiętać o tym, że to na nich ciąży obowiązek wykazania, że dysponują odpowiednią podstawą prawną do przetwarzania danych osobowych swoich użytkowników, np. kiedy wysyłają im newslettery. W razie wątpliwości administrator danych musi wykazać, że taką zgodę uzyskał. Dlatego jeśli firma buduje bazę danych użytkowników, to powinna archiwizować w niej dane o tym, kiedy i na jaki zakres przetwarzania wyraziła zgodę dana osoba.

Zgoda na przetwarzanie danych musi być wyrażona dobrowolnie i świadomie, w drodze jednoznacznej, potwierdzającej czynności. RODO mówi wyraźnie: milczenie, okienka domyślnie zaznaczone lub niepodjęcie działania nie powinny oznaczać zgody. Użytkownik podający swoje dane na stronie internetowej musi wyrazić ją świadomie i czynnie, na przykład poprzez zaznaczenie odpowiedniego pola - tak zwanego checkboksa. **Nie wystarczy zatem wyświetlić użytkownikowi informację o tym, że firma będzie przetwarzała jego dane osobowe, nie można też stosować checkboksów, które są domyślnie zaznaczone.**

Jeśli dane osobowe są zbierane w różnych celach, to przedsiębiorca musi pozyskać osobne zgody na każdy z nich. Przykładowo, jeśli chcemy rejestrować użytkowników z zamiarem wykorzystania ich danych do celów marketingowych oraz w celu opracowywania danych, powinno być to zapisane w odrębnych formułach zgód, które zostaną wyświetlone obok zgody na przetwarzanie danych. Użytkownik powinien zaznaczyć każdą z nich z osobna.

Na pytanie Interaktywnie.com odpowiedziała Agnieszka Świątek-Druś, rzecznik prasowy Urzędu Ochrony Danych Osobowych:

RODO nie stawia żadnych konkretnych wymagań co do wyglądu formularza, który miałby służyć do wyrażania zgody na przetwarzanie danych w określonym celu.

Nie można zatem wskazać jednoznacznie, jak taki formularz powinien wyglądać. Ważne jest jednak, aby w formularzu takim przed takimi elementami jak np. pola alternatywnego wyboru z opcjami „zgadzam się" lub „nie zgadzam się", za pomocą których osoba może poprzez akcję, którą musi wykonać (zaznaczenie właściwego pola), była poinformowana o wszystkich tych elementach na które wskazuje art. 13 RODO, tj. o:

- tożsamości i danych kontaktowych administratora oraz, gdy ma to zastosowanie, tożsamości i danych kontaktowych jego przedstawiciela;
- gdy ma to zastosowanie – danych kontaktowych inspektora ochrony danych;
- celu przetwarzania danych osobowych, oraz podstawie prawnej ich przetwarzania;
- jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f) – prawnie uzasadnionych interesach realizowanych przez administratora lub przez stronę trzecią;
- informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;
- gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony lub w przypadku przekazania, o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz informację o sposobach uzyskania kopii tych zabezpieczeń lub o miejscu ich udostępnienia;

- okresie, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
- prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;
- jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) – informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;
- prawie wniesienia skargi do organu nadzorczego;
- czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych;
- czy dane wykorzystywane będą do zautomatyzowanego podejmowania decyzji,

w tym do profilowania, o którym mowa w art. 22 ust. 1 i 4, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

RAPORTY INTERAKTYWNIE.COM 2019

JAK ZABEZPIECZYĆ PRZEDSIĘBIORSTWO PRZED CYBERATAKIEM?

Kaja Grzybowska
redaktor Interaktywnie.com

kg@interaktywnie.com

6

„Dlaczego polskie firmy w walce z cyberprzestępcami liczą na szczęście?" Już sam podtytuł raportu przygotowanego w 2017 roku przez analityków PwC sugerował, że - jeśli chodzi o świadomość, cybernetycznych zagrożeń - jesteśmy przekonani, że jakoś to będzie. Było jednak tak, że w 2017 roku 44% firm wskutek ataku poniosło straty finansowe, a aż 62% odnotowało zakłócenia i przestoje. Czy czegoś nas to nauczyło?

W 2017 roku spustoszenie siały WannaCry i NotPetya, których masowy zasięg związany był z najsłabszym ogniwem w łańcuchu zabezpieczeń, czyli aktywnością człowieka. W roku 2018 nie było wiele lepiej, mimo że - jak wynika z raportu przygotowanego przez specjalistów z Xopero Software - aż ponad 48% polskich przedsiębiorców zadeklarowało zwiększenie nakładów na bezpieczeństwo IT. Z danych State of SMB Cybersecurity Report wynika jednak, że aż 67% małych i średnich firm mimo wszystko doświadczyło cyberataku, a 58% naruszenia danych.

W większości przypadków przedsiębiorcy nie mieli zaplecza technologicznego, by zadbać o odpowiedni poziom zabezpieczeń, ale zważywszy na niedobór specjalistów zajmujących się cyberbezpieczeństwem, można podejrzewać, że szybko się to nie zmieni. System zabezpieczeń to system właśnie. Składa się z wielu ogniw i ich wybór każdego wymaga specjalistycznej wiedzy. Z danych zawartych w raporcie KPMG wynika, że brak wykwalifikowanej kadry jest dla 63% firm problemem, który w największym stopniu uniemożliwia budowę odpowiednich zabezpieczeń.

Dopiero na drugim miejscu jest wymieniany budżet, choć analitycy KPMG podkreślają, że firmy coraz chętniej przeznaczają dodatkowe środki właśnie na wzmocnienie cyberochrony. Z analiz IDC wynika,

że wydatki na odpowiednie rozwiązania wyniosą w 2019 roku 27,3 mld USD, wzrastając o 8,3 proc. w stosunku do ub.r.

> Cisco szacuje, że w polskich firmach brakuje ok. 5 tys. specjalistów ds. cyberbepieczeństwa. Za rok będzie to już do 10 tys. osób.
>
> *źródło: Interaktywnie.com*

Brak specjalistów od cyberbezpieczeństwa oznacza jednak, że większość ataków, których teraz doświadczamy nigdy nie zostanie nie tylko ujawniona, ale i przeanalizowana, a biorąc pod uwagę zwiększającą się liczbę urządzeń, które potencjalnie mogą stać się celem ataku, nie jest to optymistyczna prognoza.

Jak zabezpieczyć przedsiębiorstwo przed cyberatakiem?

Tam, gdzie zatrudnienie eksperta w zakresie cyberbezpieczeństwa nie wchodzi w grę, należy podjąć podstawowe działania zwiększające ochronę. Pierwszym, o którym nie wolno zapomnieć jest posiadanie aktualnego i legalnego oprogramowania. Hakerzy najczęściej bowiem wykorzystują powszechne luki najbardziej znanych systemach, ale ich producenci stale testują własny soft i na bieżąco reagują na wszystkie problemy.

Newralgicznym punktem są jednak nie tylko urządzenia podpięte do sieci, ale także sama sieć. Połączenie Wi-Fi powinno być właściwie zabezpieczone, bo - o czym wiele osób nie pamięta - w innym przypadku grozi nam nie tylko wyciek, ale także bezprawne użycie adresu IP, który może zostać wykorzystany w celach przestępczych.

Silne hasła to temat, który wraca jak bumerang za każdym razem, kiedy okazuje się, że wśród tych najczęściej stosowanych znajdują się takie perełki jak „password", „qwerty" lub „12345". Powtórzmy więc raz jeszcze, że hasła powinny być odpowiednio długie (co najmniej 8 znaków) i składać się z liter, cyfr i znaków specjalnych. Nie warto też używać informacji takich jak data urodzenia lub nazwisko panieńskie matki, bo takie typy hakerzy sprawdzają w pierwszej kolejności, przeczesując np. media społecznościowe w poszukiwaniu podobnych informacji.

Na końcu, trzeba oczywiście wspomnieć o programie antywirusowym. Eksperci od cyberbezpieczeństwa zalecają wybór płatnych, ale pojawia się też wiele darmowych, które mogą być osiągalną alternatywą. Trzeba jednak pamiętać, że żaden nie zastąp roztropności w korzystaniu z zasobów sieci. Bo o ile rzadko już nabieramy się na darmowego iPhone'a, o tyle informacja o niezapłaconej fakturze, ciągle może uśpić naszą czujność.

RODO i jego wpływ na cyberbezpieczeństwo firm

RODO w dużym stopniu odnosi się do zasad przechowywania danych osobowych. Przedsiębiorcy mogą się ograniczyć do zakupienia pancernych szaf, w których będą trzymać dokumenty i nośniki informacji. Spełnią wymagania, ale nie jest to działanie rozwojowe.

Jednym z kluczowych celów RODO było wprowadzenie zmian mających wpłynąć na sposób myślenia o ochronie danych, a nie tylko „podrasowanie" narzędzi. Za błędy w przechowywaniu danych, odpowiedzialny jest przede wszystkim człowiek, jego świadomość i dbałość. Rozporządzenie RODO dyscyplinuje w zakresie odpowiedzialności, wymieniając cały wachlarz kar dla tych, którzy nie planują poddać się temu procesowi w odpowiedni sposób.

Problemy ze spełnieniem wymogów RODO, generuje również dług technologiczny (technologiczne zapóźnienie). Często w firmach nie do końca było wiadomo, jak ruszyć wszystkie „nagromadzone" technologie, żeby nie „zawaliła się" cała struktura informatyczna. Właśnie konsekwencji tego problemu najczęściej obawiali się przedsiębiorcy, z którymi prowadziłam rozmowy o ochronie danych.

RODO, to impuls do tego, aby zadbać o ochronę danych nie tylko doraźnie, ale też na przyszłość. Wielu przedsiębiorców wspomina w rozmowach, że chcieliby prowadzić swoje biznesy „as usual" (jak dotychczas), ale czy to jeszcze możliwe, gdy wszystko dynamicznie się zmienia ? Sami też oczekują zmian … ma być szybko, nowocześnie, bezpiecznie i tanio. Ale jak to zrobić ? Wybór tanich, niesprawdzonych lub darmowych „zabezpieczeń", kończy się ostatecznie na złych doświadczeniach np. z wirusami szyfrującymi dane i żądaniami okupu w zamian na ich odzyskanie, czy też nieskuteczną ochroną przed innymi atakami hakerskimi.

Wejście w życie RODO dało firmom szansę na zweryfikowanie swoich procedur, dokumentacji, systemów informatycznych, zabezpieczeń infrastruktury IT oraz kompetencji osób, które się tym zajmują. Na co dzień się tego nie robi na taką skalę. RODO zainicjowało dyskusję o tym, jakie mamy skuteczne narzędzia, a czego nam brakuje, aby stworzyć bezpieczne warunki przechowywania danych.

RODO już jest i w związku z tym przedsiębiorcy mają nowe zadania. Jednym z nich jest potrzeba wprowadzania spójnych rozwiązań, które długoterminowo zabezpieczą przechowywane dane. Kolejnym, powinna być większa otwartość na dyskusję o nowych technologiach i nowych dostawcach, którzy specjalizują się w przechowywaniu danych i dają gwarancję na świadczone przez siebie usługi. Ochrona danych w cyberprzestrzeni nie może być realizowana przez jedną osobę zatrudnioną w dziale IT. Sprawa jest na tyle poważna, że tą odpowiedzialność ceduje się na firmy, które się w tym specjalizują. Nie wystarczy już zastosowanie tego samego podejścia jak dotychczas, żeby długofalowo spełnić wymagania w zakresie ochrony danych. W cyfrowym świecie każdego dnia rośnie liczba ataków, które mają na celu wejście w posiadanie danych, w sposób nieuprawniony. Dobrym i bezpiecznym rozwiązaniem w zakresie ich ochrony jest prywatna chmura obliczeniowa. Usługa ta jest świadczona przez profesjonalne serwerownie (Centra Przetwarzania Danych), których w naszym kraju jest kilkadziesiąt. Takie podejście gwarantuje, że przedsiębiorca zawsze będzie wiedział, w jakim konkretnym miejscu są przechowywane jego dane, a nie jak to jest w przypadku np. chmur publicznych, że dane przechowywane są „gdzieś" na świecie. Poza tym, z polskim dostawcą prywatnej chmury, przedsiębiorca może omówić specyfikę swojego biznesu i podjąć decyzję o wprowadzeniu dodatkowych rozwiązań zabezpieczających. Nie należy mieć oporów przed korzystaniem z takich usług, ponieważ to dostawca przejmuje na siebie znaczną odpowiedzialność za stosowane zabezpieczenia, mając do tego odpowiednie narzędzia i często ogromne doświadczenie.

Jola Uździcka
Dyrektor Sprzedaży i Marketingu w Sinersio Polska Sp. z o.o.

Bezpieczne hasła wśród internautów

- tylko połowa Europejczyków (51%) używa innego hasła dla każdej strony internetowej,
- reszta osób (49%) używa kilku, tych samych haseł dla różnych stron,
- wyjątkowo dobrze na tym tle wypadają polscy internauci, aż 63% z nich deklaruje, że ma inne hasło dla każdej strony.

Nieco gorzej sytuacja wygląda, jeżeli chodzi o skłonność do zmiany hasła.

- 31% Europejczyków rzadko lub nigdy nie zmienia swoich haseł.
- Najgorzej w zestawieniu wypadają Włosi (42% z nich nie zmienia haseł)
- i Polacy (33%).
- Najlepszy wynik mają Belgowie – haseł nie zmienia tylko 21% internautów.

źródło: Interaktywnie.com

Podejrzane maile, czyli wszystkie, które pochodzą z nieznanych źródeł, trzeba traktować z dużym sceptycyzmem, ale i to nie wystarczy. Z rozwagą należy korzystać również ze stron, które odwiedzam, bo jak - podają analitycy Kaspersky Lab - w ostatnim czasie liczba ataków phishingowych wykorzystujących strony udających portale społecznościowe znacznie wzrosła.

Ataki na internautów

Na początku 2018 r. oszuści najchętniej wykorzystywali wizerunek Facebooka - podrabiane strony służyły do kradzieży danych osobowych za pośrednictwem ataków phishingowych.

Zjawisko to wpisuje się w długotrwały trend:

- w 2017 r. Facebook znalazł się wśród trzech najpopularniejszych firm, których wizerunek był wykorzystywany w cyberatakach (z udziałem wynoszącym prawie 8%),
- wyprzedzając firmę Microsoft (6%)
- oraz PayPal (5%).

Przyczyną tak dużej popularności Facebooka wśród cyberprzestępców jest prawdopodobnie 2,13 miliarda aktywnych użytkowników miesięcznie na całym świecie, wśród których znajdują się również tacy, którzy logują się do nieznanych aplikacji przy pomocy danych uwierzytelniających do Facebooka, udzielając tym samym dostępu do swoich kont. W ten sposób nieostrożni użytkownicy Facebooka stają się lukratywnym celem cyberprzestępczych ataków phishingowych.

źródło: Interaktywnie.com

Inwestować w software czy w edukację pracowników?

Liczba urządzeń podłączonych do sieci rośnie, podobnie jak liczba przetwarzanych danych, ale jedno nie zmieniło się od lat - najsłabszym ogniwem w systemów zabezpieczeń w firmach jest w dalszym ciągu człowiek. Dane Cisco wskazują, że odpowiada on za 48% wszystkich przypadków naruszeń.

Tym samym, zmiana postaw pracowników jest dla firm najważniejszym wyzwaniem. Pracownicy wciąż otwierają nieznane załączniki, które przychodzą na ich skrzynki mailowe, a każdy może skutkować stratami dla firmy. Powinni więc być zapoznani z obowiązującą polityką bezpieczeństwa, a także regularnie aktualizować wiedzę np. w ramach cyklicznych szkoleń czy warsztatów. Informacje na temat największych zagrożeń i ich potencjalnych skutków powinny być powtarzane tak, żeby stały się częścią biurowej rzeczywistości, a nie kolejnym abstrakcyjnym wymysłem HR-u.

Bez inwestycji w edukację pracowników, inwestycja w systemu IT nie przyniesie spodziewanych korzyści. Nie można jednak zaniedbywać ani jednego, ani drugiego, a wszelkie działania - warto poprzedzić konsultacjami.

Nie ma bowiem jednej uniwersalnej recepty na bezpieczeństwo, a już sam wybór odpowiedniego systemu nastręcza trudności. Jest ich bowiem mnóstwo, mogą przeciwdziałać zagrożeniom, wykrywać je albo jedynie reagować, ale nie sposób wskazać jednego, który zajmie się wszystkim. System bezpieczeństwa składa się z wielu połączonych ze sobą elementów i zanim zdecydujemy się na wybór konkretnych, trzeba zorientować się dokładnie, czego potrzebujemy.

Dobrym pomysłem jest przeprowadzenie w tym celu audytu. Z obserwacji Deloitte wynika, że na współpracę z zewnętrznymi konsultantami od cyberbezpieczeństwa decyduje się coraz więcej firm.

Chmura remedium na atak?

Według IDC, w skali globalnej, aż 9/10 firm korzysta z cloud computingu, a do 2025 roku biznes umieści w chmurze 60% swoich danych, choć - jak zauważają analitycy Xopero Software w raporcie Cloud Computing - statystyki są zawyżone są przez firmy, które korzystają wyłącznie z podstawowych usług w chmurze, takich jak poczta mailowa czy programy do przechowywania i współdzielenia dokumentów.

Specjaliści podkreślają, że niewiele firm może pozwolić sobie na tak zaawansowane zabezpieczenia, jakie stosują firmy oferujące usługi chmurowe, ale to właśnie obawa o bezpieczeństwo długo była największą barierą powstrzymującą przedsiębiorców przed lokowaniem tam danych. Oczywiście, chmura sama w sobie nie jest żadną gwarancją, ale - jeśli nasze dane spoczywają na serwerach Google, Microsoftu czy Amazona - można podejrzewać, że ich ochrona będzie na odpowiednio wysokim poziomie.

Zawsze jednak warto sprawdzić, jak kwestie bezpieczeństwa traktują konkretni usługodawcy, zwracając uwagę na certyfikaty ISO. Zwłaszcza istotny wydaje się standard ISO 27018, który jest kodeksem postępowania związanym z ochroną danych osobowych w chmurach obliczeniowych czy ISO/IEC 27017 określający praktyki dotyczące środków kontroli bezpieczeństwa.

A może blockchain?

Blockchain, czyli technologia stojąca u podstaw kryptowalut, długo przez piewców tego rozwiązania, uznawana była za system niemalże kuloodporny. Dzisiaj już tak nie jest, a blockchain coraz częściej staje się celem ataków cyberprzestępców. Ofiarami ataków padły m.in. oparte na blockchainie platformy DAO, serwis crowdfundingowy, który umożliwiał wspieranie innowacji za pomocą kryptowaluty i Bitfinex, kantor do wymiany walut wirtualnych.

Rodzaje usług dostępnych w chmurze:

- SaaS, czyli Software as a Service, z angielskiego oprogramowanie jako usługa, polega na udostępnianiu przez internet oprogramowania bez konieczności instalowania go na dysku komputera. Dostawca usługi dba o jego aktualizację i poprawność działania. SaaS może stanowić aż 62 proc. polskiego rynku.
- IaaS, czyli Infrastructure as a Service, z angielskiego infrastruktura jako usługa. Dostawca zapewnia klientowi infrastrukturę, np. miejsce na serwerach. Nie dostarcza mu jednak fizycznie serwerów, ale oferuje odpowiednią przestrzeń na swoich urządzeniach. Dużą zaletą jest tutaj skalowanie w zależności od potrzeb. Np. sklep internetowy musi być gotowy na większy ruch podczas przedgwiazdkowych zakupów – dostawca usługi zapewnia mu wtedy większą wydajność infrastruktury. IaaS jest w 28 proc. odpowiedzialny za przychody z cloud computingu.
- PaaS, czyli Platform as a Service, z angielskiego platforma jako usługa. Dostawca usługi oferuje wirtualne środowisko pracy składające się z różnych programów, aplikacji itp. Np. programista nie musi kupować licencji różnych programów, może stworzyć aplikację na dowolnym sprzęcie używając przeglądarki internetowej. Całe zaplecze jest w chmurze. Jeden złoty z dziesięciu jest wydawany w Polsce na PaaS.

źródło: Interaktywnie.com

Robert Grabowski, kierownik CERT z Orange Polska już w 2018 roku podkreślał jednak, że zwykle winna była nie sama technologia, ale jej implementacja, a zalety samego blockchaina ciągle są niepodważalne i wynikają wprost z koncepcji decentralizacji usług i sposobu uwierzytelnienia stron transakcji opartych na konsensusie.

Analitycy IDC spodziewają się więc, że wydatki na blockchain będą rosnąć i to w tempie 80,2 proc. rdr w samej tylko Europie, która jest drugim co do wielkości rynkiem dla tej technologii.

O REDAKCJI

Redakcja

Tomasz Bonek
prezes zarządu i redaktor naczelny
tb@interaktywnie.com

Paweł Musiał
redaktor Interaktywnie.com
pm@interaktywnie.com

Robert Cieszawski
redaktor Interaktywnie.com
rc@interaktywnie.com

Barbara Chabior
redaktor Interaktywnie.com
bch@interaktywnie.com

Kaja Grzybowska
redaktor Interaktywnie.com
kg@interaktywnie.com

Przemysław Ławrowski
redaktor Interaktywnie.com
pl@interaktywnie.com

Reklama

Jakub Karczmarczyk
sales director
+48 693 710 118, +48 71 302 75 35
jk@interaktywnie.com

O INTERAKTYWNIE.COM

Adres i siedziba redakcji

interaktywnie.com

Interaktywnie.com sp. z o.o.
ul. Oławska 17 lok. 6 - III piętro
50-123 Wrocław
tel.: 71-302-75-35
redakcja@interaktywnie.com

NIP: 898-215-19-79
REGON: 020896541

Spółka zarejestrowana we Wrocławiu, kod pocztowy 50-302, przy ul. Jedności Narodowej 152/177, przez Sąd Rejonowy dla Wrocławia-Fabrycznej we Wrocławiu, VI Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS 0000322917

Kapitał zakładowy 6 000,00 zł

Interaktywnie.com to specjalistyczny magazyn dla wszystkich pracujących w branży internetowej oraz tych, którzy się nią pasjonują. Serwis zintegrował także społeczność, klika tysięcy osób, które wymieniają się tu doświadczeniami, doradzają sobie, piszą blogi, rozmawiają o najnowszych rozwiązaniach.

Interaktywnie.com istnieje od 2006 roku, na początku był branżowym blogiem. W ciągu trzech pierwszych lat znacząco poszerzył się zarówno zakres tematyczny jaki i liczba autorów, którzy w nim publikują. Zostało to docenione przez jury WebstarFestival i uhonorowane statuetką Webstara Akademii Internetu. Oprócz tego wortal jest laureatem Grand Webstara 2008 dla strony roku.

Dziś Interaktywnie.com to nowoczesne internetowe medium tematyczne z codziennie nowymi newsami z rynku polskiego i międzynarodowego, artykułami, wywiadami oraz omówieniami najciekawszych stron internetowych.

Jego redakcja przygotowuje też cykliczne, obszerne raporty branżowe, dystrybuowane do najlepszej grupy odbiorców. Wśród nich są specjaliści zarejestrowani w Interaktywnie.com. Są to szczegółowe opracowania dotyczące poszczególnych segmentów rynku internetowego i zmian, które na nim zachodzą.

Raporty promowane są także każdorazowo w największych polskich serwisach: wp.pl, gazeta.pl, interia.pl.
Więcej raportów: www.interaktywnie.com/biznes/raporty

Wykorzystane do raportu zdjęcia pochodzą z banku zdjęć Pixabay.