FORTINET

BEZPIECZEŃSTWO DANYCH W ŚWIETLE RODO — JAK PRZYGOTOWAĆ SIĘ NA NIEUNIKNIONE

SPIS TREŚCI

WSTĘP

Przyjęte przez Unię Europejską ogólne rozporządzenie o ochronie danych (RODO), które ma zastosowanie od 25 maja 2018 r., radykalnie zwiększa sankcje za niewłaściwą ochronę danych osobowych użytkowników. Maksymalne kary pieniężne z tego tytułu będą znacznie wyższe od dotychczasowych i sięgną czterech procent globalnych przychodów przedsiębiorstwa naruszającego przepisy RODO albo 20 mln EUR, w zależności od tego, która z tych kwot jest wyższa.

Mimo tak wysokich kar RODO daje przedsiębiorstwom jedynie nieliczne wytyczne dotyczące ***sposobu*** przestrzegania zawartych w nim przepisów. Nie ma jednak powodu do paniki. Jeśli nawet przedsiębiorstwo zostanie uznane za nieprzestrzegające przepisów RODO, nadal ma możliwość obniżenia albo wręcz uniknięcia grożących mu kar, o ile wykaże, że podejmowało dobre decyzje dotyczące przetwarzania danych osobowych. Ma to zastosowanie zwłaszcza w przypadku potencjalnego naruszenia ochrony danych.

Wdrożenie proaktywnych i dobrze przemyślanych zasad i procedur w zakresie ochrony danych może zabezpieczyć przedsiębiorstwo nie tylko przed sankcjami przewidzianymi w przepisach RODO, ale również przed prawnymi i wizerunkowymi skutkami naruszenia ochrony danych. Wzmacnianie procesów związanych z zapobieganiem utracie danych i wykrywaniem zagrożeń jest zatem ważniejsze niż kiedykolwiek.

Podczas przygotowywania lub rozwijania zasad ochrony danych przedsiębiorstwa muszą pamiętać, że:

- włamania są nieuniknione;
- architektura zabezpieczeń może wymagać pseudonimizacji i segmentacji;
- nowoczesne zabezpieczenia to podstawa.

1 WŁAMANIA SĄ NIEUNIKNIONE

W kontekście ochrony danych nic nie jest pewne. W miarę doskonalenia zabezpieczeń korporacyjnych przez firmy zajmujące się bezpieczeństwem informatycznym, przestępcy niestrudzenie próbują być o krok naprzód. Są przy tym coraz bardziej kreatywni, a zachęt do tworzenia innowacyjnych rozwiązań im nie brakuje.

Obecna złożoność i szybkość przeprowadzania ataków oznacza, że bez względu na kwoty wydawane przez przedsiębiorstwa na bezpieczeństwo informatyczne, można co najwyżej zmniejszyć, a nie wyeliminować prawdopodobieństwo włamania do sieci wewnętrznej. Oprócz przeznaczenia odpowiednich zasobów na zapobieganie zagrożeniom, przedsiębiorstwa powinny zatem również rozważyć sposoby pozwalające na ograniczenie skutków włamań, jeśli już do nich ewentualnie dojdzie.

Cyberprzestępca, który narusza sieć przedsiębiorstwa, ma średnio 65 dni na dokonanie spustoszeń, zanim fakt takiego włamania zostanie wykryty[1]. Im dłużej takie „okno możliwości" jest otwarte, tym więcej czasu przestępca może poświęcić na wyszukanie, znalezienie i kradzież ważnych danych. Z drugiej strony im szybciej przedsiębiorstwo wykryje zagrożenie, tym większe ma szanse na ograniczenie jego skutków albo nawet zapobieżenie takiemu zagrożeniu.

Elementem programu zapewnienia bezpieczeństwa informatycznego w każdym przedsiębiorstwie musi być zatem skupienie się na minimalizacji okresu upływającego od momentu dokonania do momentu wykrycia i usunięcia skutków naruszenia ochrony danych. W tym kontekście zadania osoby odpowiedzialnej za bezpieczeństwo informatyczne są następujące:

[1] „2017 Trustwave Global Security Report" (Raport Trustwave z 2017 r. o bezpieczeństwie globalnym), czerwiec 2017 r.

ZROZUMIENIE TYPÓW DANYCH ZBIERANYCH I PRZECHOWYWANYCH PRZEZ PRZEDSIĘBIORSTWO

Każde przedsiębiorstwo powinno starannie zbadać, jakie dane osobowe zbiera lub w inny sposób przetwarza. Czy dane te należą do rezydenta UE? Jeśli tak, przedsiębiorstwo powinno określić, czy korzysta z tych danych w pierwotnie wskazanych celach oraz czy musi te dane nadal zbierać lub przechowywać.

Jeśli odpowiedzi na te pytania są twierdzące, wówczas przedsiębiorstwo musi zbadać, gdzie przechowuje, jak chroni oraz jak przesyła między swoimi systemami takie dane osobowe, a także jak je ewentualnie przekazuje osobom trzecim.

PRZYGOTOWANIE SIĘ NA NIEUNIKNIONE

Jeśli przedsiębiorstwo wykryje naruszenie ochrony danych osobowych objęte przepisami RODO, ma 72 godziny na zgłoszenie tego faktu właściwemu organowi nadzorczemu, chyba że „jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych". Oznacza to, że w ciągu trzech dni przedsiębiorstwo musi określić, czyich danych osobowych dotyczyło naruszenie, jakie dane osobowe zostały narażone na zagrożenie oraz jaki jest stopień potencjalnego wpływu tego naruszenia na określone osoby fizyczne.

Wymogi zgłaszania naruszeń ochrony danych osobowych są wzmocnione w przypadku, gdy dane naruszenie „może

powodować ***wysokie*** ryzyko naruszenia praw lub wolności osób fizycznych". W takim przypadku przedsiębiorstwo musi również powiadomić o tym naruszeniu rezydentów UE, których dane zostały narażone na zagrożenie.

Aby spełnić te wymogi, przedsiębiorstwo, które wykryło naruszenie ochrony danych, musi bardzo szybko określić systemy, do których dostał się haker. Zazwyczaj konieczne jest wówczas zbadanie ruchu sieciowego oraz sprawdzenie poszczególnych urządzeń i aplikacji.

[2] Ogólne rozporządzenie o ochronie danych, art. 33: „Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu".

[3] Ogólne rozporządzenie o ochronie danych, art. 34: „Zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych".

Oprócz konieczności zestawienia informacji niezbędnych do zgłoszenia przypadku naruszenia ochrony danych, zespół IT musi dowiedzieć się, w jaki sposób przestępca dostał się do sieci wewnętrznej. Jeśli się tego dowie, możliwe będzie zapobieżenie ewentualnym przyszłym próbom naruszeń, a także upewnienie się, że haker nie ma już dostępu do takiej sieci. Istotne dla przedsiębiorstwa jest również pełne zrozumienie celu i skutków wspomnianego naruszenia, aby uzyskać pewność, że zgłoszenie przekazywane do właściwego organu ochrony danych lub osoby, której dane dotyczą, zawiera rzetelne informacje. Jeśli natomiast przedsiębiorstwo nie zgłasza przypadku naruszenia ochrony danych podmiotom zewnętrznym, musi uzyskać całkowitą pewność, że przepisy RODO zezwalają na niezgłoszenie takiego przypadku.

Tak czy inaczej zdolność do szybkiej reakcji ma charakter kluczowy. W rzeczywistości przedsiębiorstwo, które szybko reaguje na przypadki naruszenia zabezpieczeń swojej sieci, może w takim stopniu powstrzymać taki atak, aby zminimalizować jego potencjalne skutki w kontekście RODO.

Przedsiębiorstwa muszą mieć starannie udokumentowane plany reagowania na incydenty obejmujące procedury wykrywania i badania przypadków włamania do sieci. Należy tam określić osoby zaangażowane w poszczególne procesy na wypadek naruszenia ochrony danych. Zazwyczaj w reakcję na takie incydenty zaangażowany jest dyrektor ds. zabezpieczeń informatycznych, radca prawny przedsiębiorstwa oraz członek ścisłego kierownictwa przedsiębiorstwa. Zadaniem tej ostatniej osoby jest podjęcie ostatecznej decyzji co do oficjalnej reakcji przedsiębiorstwa na taki przypadek naruszenia.

Ponadto takie plany wykrywania zagrożeń i reagowania na incydenty, podobnie jak wszelkie procesy związane z cyberprzestępczością, muszą być systematycznie testowane.

WDROŻENIE W PRZEDSIĘBIORSTWIE ODPOWIEDNICH PROCESÓW I ROZWIĄZAŃ DO TWORZENIA I ODZYSKIWANIA KOPII ZAPASOWYCH DANYCH

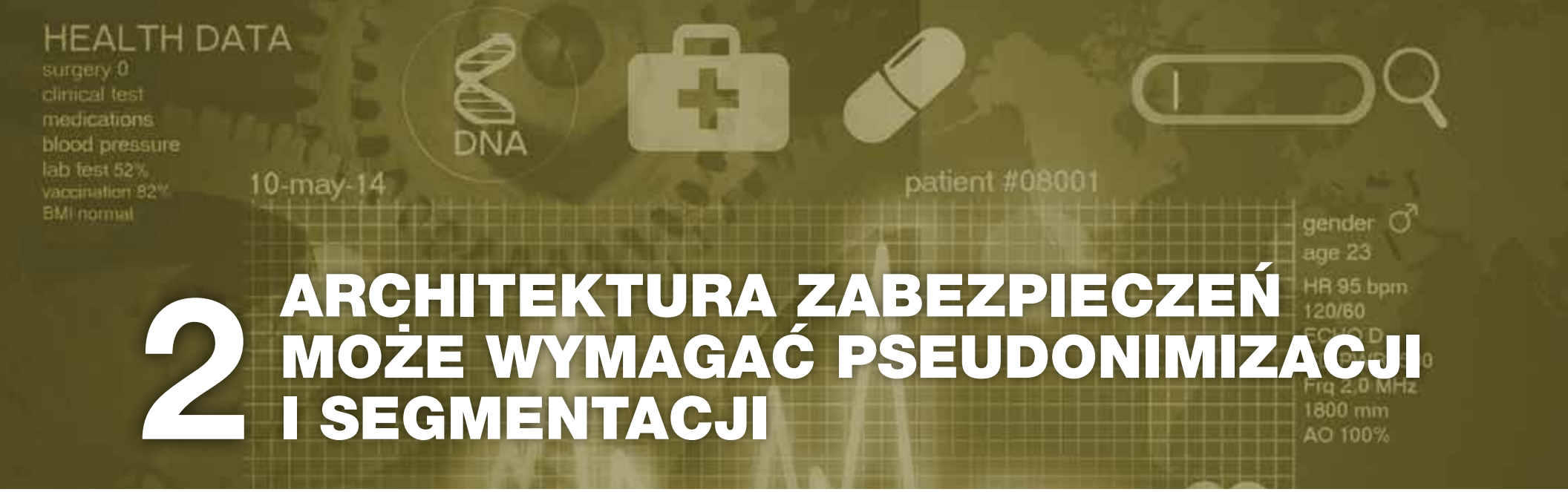
Wdrożenie dobrego rozwiązania do tworzenia i odzyskiwania kopii zapasowych danych w odniesieniu do wszystkich kluczowych systemów przedsiębiorstwa to kolejny niezbędny element przygotowań na potencjalne włamania do sieci. Odzyskane pliki mogą okazać się przydatne w wykryciu ścieżki ataku oraz mogą okazać się bezcenne w przypadku ataku dokonanego za pomocą oprogramowania szyfrującego w celu wymuszenia okupu (ang. ransomware attack), w ramach którego przestępcy grożą, że jeśli nie otrzymają okupu, trwale zniszczą zaszyfrowane i wyeksportowane dane przedsiębiorstwa.

SKOORDYNOWANIE DZIAŁANIA WSZYSTKICH SYSTEMÓW I PROCESÓW W RAMACH CAŁEJ POWIERZCHNI ATAKU

Skuteczność działania funkcji zapobiegania przypadkom i wykrywania przypadków zagrożeń zależy od odpowiedniej koordynacji planów, procesów i informacji w ramach całej sieci przedsiębiorstwa. Brak takiej koordynacji w połączeniu ze złożonością, zwłaszcza w kontekście infrastruktury zabezpieczeń sieci, osłabiają zdolność przedsiębiorstwa do wykrywania przypadków i reagowania na przypadki naruszenia bezpieczeństwa. Sytuacja jest jeszcze gorsza wówczas, gdy aktualizacje danych o zagrożeniach pochodzą od rożnych partnerów. Jedna poprawka systemu może od razu zablokować konkretny atak, podczas gdy inna poprawka może nie zawierać jeszcze przez kilka kolejnych tygodni żadnych informacji o tym ataku.

Jednym z najważniejszych działań, które osoba odpowiedzialna za zabezpieczenia IT może podjąć na wypadek potencjalnego naruszenia bezpieczeństwa, jest ocena poziomu zintegrowania ze sobą wdrożonych w przedsiębiorstwie systemów zabezpieczeń. Wiele przedsiębiorstw korzysta ze zróżnicowanych technologii zabezpieczeń, z których każda wykonuje określone funkcje w ramach infrastruktury zabezpieczeń. Problemem jest jednak to, że wspomniane technologie nie zostały zaprojektowane do współpracy ze sobą. Oznacza to, że dział IT widzi zagrożenia w ramach poszczególnych silosów, ale brakuje mu ogólnej perspektywy obejmującej całość powierzchni ataku. Tymczasem proces agregacji danych z takich silosów wymaga czasu i jest obarczony ryzykiem błędów.

Hakerzy mogą zatem wykorzystać taką niedostateczną widoczność tych systemów zabezpieczeń. Ponadto jeśli do wykrycia naruszenia ochrony danych jednak dojdzie, wspomniany brak integracji między danymi i systemami w jeszcze większym stopniu utrudni określenie, czy takie naruszenie powinno zostać zgłoszone na mocy przepisów RODO. Ze wszystkich powyższych względów przedsiębiorstwa potrzebują takiej infrastruktury zabezpieczeń informatycznych, której wszystkie elementy wymieniają się informacjami o zagrożeniach i zapewniają dobrą widoczność w czasie rzeczywistym.



2 ARCHITEKTURA ZABEZPIECZEŃ MOŻE WYMAGAĆ PSEUDONIMIZACJI I SEGMENTACJI

Oprócz oceny stopnia integracji systemów zabezpieczeń w ramach całej infrastruktury sieci przedsiębiorstwa, osoby odpowiedzialne za bezpieczeństwo informatyczne, które chcą przygotować się na przepisy RODO, muszą rozważyć kwestie tego, czy i jak dane są szyfrowane i przechowywane w sieci przedsiębiorstwa.

Niektóre przedsiębiorstwa chronią dane osobowe w drodze ich anonimizacji, czyli procesu, który trwale usuwa z nich pierwiastek powiązania z konkretną osobą. Na przykład placówka ochrony zdrowia może wymazać z dokumentacji medycznej imiona i nazwiska pacjentów, wskutek czego dokumentacji tej nie będzie można w żaden sposób powiązać z konkretnym pacjentem. Jest to skuteczny sposób na usuwanie danych osobowych ze względu na potrzebę ich ochrony przez dział IT, ale stwarza on również określone problemy w przypadku, gdyby w przyszłości placówka taka musiała odzyskać dane konkretnego pacjenta. Zanonimizowane dane nigdy nie mogą zostać bowiem przywrócone do pierwotnego stanu.

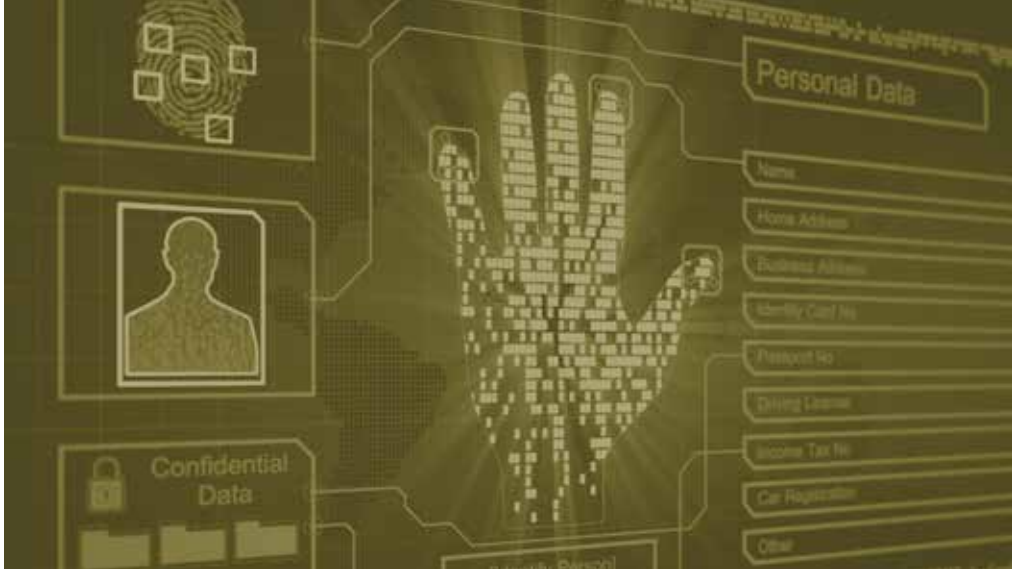
Alternatywnym rozwiązaniem jest w tym przypadku pseudonimizacja, czyli proces zastępowania identyfikatorów osobowych, takich jak imiona i nazwiska, ciągami odwracalnych, spójnych znaków służących za pseudonim. Za klucz służy oddzielny plik, który zestawia poszczególne identyfikatory osobowe z przypisanymi im pseudonimami. Jeśli haker miałby uzyskać dostęp do poddanej pseudonimizacji dokumentacji medycznej, nic w niej obecne nie byłoby powiązane z konkretnym pacjentem. Aby dokonać takiego powiązania, haker musiałby zatem również zdobyć plik z kluczem.

PSEUDONIMIZACJA TO KLUCZ DO WYGODNIEJSZEGO ZAPEWNIENIA BEZPIECZEŃSTWA

W rzeczywistości ogólne rozporządzenie o ochronie danych uznaje pseudonimizację za jeden z odpowiednich środków technicznych i organizacyjnych, [które przedsiębiorstwa mogą wdrożyć], aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku”[4]. Wdrożenie pseudonimizacji może również zademonstrować odpowiedniemu organowi ochrony danych (w przypadku naruszenia ochrony danych), że dane przedsiębiorstwo podjęło istotne działania mające na celu zminimalizowanie skutków tego naruszenia dla właścicieli danych. Wymogi dotyczące zgłoszeń przypadków naruszenia ochrony danych na mocy RODO są również mniej uciążliwe dla przedsiębiorstw, które stosują pseudonimizację, niż dla przedsiębiorstw, które przechowują dane osobowe w formie zwykłego tekstu, ponieważ pseudonimizacja minimalizuje prawdopodobieństwo utraty danych osobowych.

SEGMENTACJA SIECI CHRONI KLUCZE PRZED KRADZIEŻĄ

Po utworzeniu plików służących jako klucz do odszyfrowania poddanych pseudonimizacji dokumentów należy te pliki od nich oddzielić, czyli umieścić je w oddzielnych segmentach sieci przedsiębiorstwa. Ponadto powinno się jeszcze lepiej zabezpieczyć te segmenty sieci w drodze wdrożenia tam wewnętrznych



zapór, aby zapobiec możliwości przemieszczania się potencjalnego hakera między segmentami.

Przedsiębiorstwo może na przykład przechowywać dokumentację pracowniczą w systemie działu kadr, ale poddać ją pseudonimizacji tak, aby żaden z dokumentów nie mógł zostać powiązany z konkretnym pracownikiem. Klucze służące do odszyfrowania danych osobowych pracowników mogłyby być wówczas przechowywane w systemie działu finansowego. Między systemami obu tych działów należałoby wówczas wdrożyć odpowiednią zaporę w sieci wewnętrznej. Nawet jeśli cyberprzestępca uzyskałby dostęp do segmentu sieci z danymi z działu kadr, nie mógłby wtedy odszyfrować znajdującej się tam dokumentacji pracowniczej bez uzyskania dostępu do segmentu sieci z danymi działu finansowego, a zapora wewnętrzna znacznie ograniczyłaby jego zdolności do poruszania się między tymi dwoma segmentami sieci.

[4] Ogólne rozporządzenie o ochronie danych, art. 32: „Bezpieczeństwo przetwarzania”.

3 NOWOCZESNE ZABEZPIECZENIA TO PODSTAWA

Przepisy RODO również zachęcają przedsiębiorstwa do wdrażania nowoczesnych (uwzględniających stan wiedzy technicznej) technologii zabezpieczeń. Art. 25 stwierdza, że **„uwzględniając stan wiedzy technicznej, … 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…”**[5].

Przedmiotowe rozporządzenie nie definiuje pojęcia „uwzględniające stan wiedzy technicznej”, ale wyraźnie wskazuje, że objęta jest nim pseudonimizacja. Określenie, które technologie można uznać za nowoczesne, po prostu ewoluuje w miarę jak ewoluuje rynek rozwiązań IT. Na dzień dzisiejszy uzasadnione wydaje się zatem założenie, że w celu zapewnienia odpowiedniej ochrony przesyłanych i przechowywanych danych przedsiębiorstwo musi korzystać z nowoczesnych technologii.

[5] Ogólne rozporządzenie o ochronie danych, art. 25: „Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych”.

Złożoność nie tylko utrudnia wykrywanie zagrożeń, ale jest również zaprzeczeniem nowoczesnej technologii. Poszczególne funkcje zabezpieczeń nie mogą bowiem działać w silosach. Ich integracja jest niezbędna zarówno do zapewnienia skutecznego działania całej infrastruktury zabezpieczeń informatycznych, jak i do spełnienia określonego w RODO wymogu stosowania nowoczesnych rozwiązań. Podobnie automatyzacja działań zmierzających do ograniczenia zagrożeń jest niezbędna zarówno do zabezpieczenia przedsiębiorstwa, jak i do spełnienia wspomnianego wymogu.

Bieżąca ocena ryzyka jest również nieodzowna. Mechanizmy automatycznie wykorzystujące informacje o zagrożeniach przyczyniają się do zmniejszenia ryzyka kradzieży danych oraz nałożenia kary na przedsiębiorstwo, gdy do takiej kradzieży jednak dojdzie. Aby jednak mieć możliwość zapobiegania cyberatakom, mechanizmy te muszą otrzymywać aktualizowane na bieżąco informacje o zagrożeniach.

PODSUMOWANIE

Do momentu rozpoczęcia stosowania przepisów RODO nikt tak właściwie nie wie, jak poszczególne kraje będą te przepisy egzekwować. Brytyjski urząd komisarza ds. informacji (Information Commissioner's Office, ICO)[6] udostępnia więcej przydatnych informacji na ten temat, w tym słowa komisarza ds. informacji, Elizabeth Denham, która we wpisie na blogu stwierdza, że „sianiem paniki jest sugerowanie, że od początku będziemy przykładnie karać przedsiębiorstwa za drobne naruszenia albo że kary maksymalne staną się normą"[7]. O ile zatem RODO stanie się „prawem krajowym" mającym na celu raczej ochronę danych niż szczegółową analizę stosowanych technologii, o tyle skieruje ono uwagę na wszystkie aspekty dotyczące filozofii i stanowiska przedsiębiorstwa w kwestii bezpieczeństwa.

Nie czas zatem na panikę. Każde przedsiębiorstwo na świecie, które przetwarza dane osobowe rezydentów UE, musi teraz ponownie ocenić swoją infrastrukturę zabezpieczeń informatycznych. Czy stosowane w jej ramach rozwiązania są nowoczesne? Czy obejmuje ona zaawansowane technologie ochrony danych, w tym mechanizmy zapobiegania przypadkom i wykrywania przypadków zagrożeń, pseudonimizacji i segmentacji sieci wewnętrznej? Czy odpowiednio udokumentowane i przetestowane zostały plany reagowania na incydenty naruszenia ochrony danych? Czy wszystkie systemy zabezpieczeń informatycznych są zintegrowane ze sobą w sposób pozwalający na optymalną ochronę danych i zapewnienie odpowiedniej widoczności całej sieci przedsiębiorstwa?

Jeśli osoby odpowiedzialne za bezpieczeństwo informatyczne przedsiębiorstwa mogą odpowiedzieć twierdząco na wszystkie te pytania, są wówczas niemal na pewno dobrze przygotowane na nieuniknione.

[6] Information Commissioner's Office (ICO)

[7] Elizabeth Denham, „GDPR—sorting the fact from the fiction", 9 sierpnia 2017 r.

www.fortinet.com

Copyright © 2017 Fortinet, Inc. Wszelkie prawa zastrzeżone. 12.14.17

143874-C-0-EN