Ochrona danych i cyberbezpieczeństwo po wprowadzeniu RODO

#KingstonIsWithYou

Ochrona danych i cyberbezpieczeństwo po wprowadzeniu RODO

Wstęp

Liczne firmy i organizacje ciężko pracowały - i intensywnie zatrudniały personel - aby przygotować się na wejście RODO. Być może twoja firma także. Jednak ciągle zmieniająca się natura cyberataków oznacza, że nie możesz sobie pozwolić na zatrzymanie się i złapanie oddechu. Zgodność z RODO nie jest celem samym w sobie, ale wytyczną, dzięki której można oceniać bieżące działania w zakresie ochrony danych i cyberbezpieczeństwa. W tej dziedzinie nie ma miejsca na samozadowolenie.

W tym krótkim eBooku gromadzimy wiedzę kilku najbardziej doświadczonych brytyjskich specjalistów z zakresu cyberbezpieczeństwa, aby omówić zmiany w ochronie danych, jakie zaszły od czasu wprowadzenia RODO. Podajemy także, w jaki sposób firmy edukują swoich pracowników w zakresie przestrzegania przepisów oraz opowiadamy, jak działy IT i dostawcy technologii mogą lepiej zabezpieczyć infrastrukturę IT i uczyć użytkowników wiedzy w zakresie pojawiających się wyzwań związanych z bezpieczeństwem.

Ochrona danych i cyberbezpieczeństwo po wprowadzeniu RODO

Współautorzy

Ten krótki eBook został opracowany przez pięciu ekspertów z dziedziny ochrony danych i cyberbezpieczeństwa.

Rob Allen
@Rob_A_kingston

Rob jest dyrektorem ds. Marketingu i usług technicznych w Kingston Technology i jest związany z firmą od 1996 roku. W swojej roli Rob jest odpowiedzialny za nadzorowanie PR, mediów społecznościowych, channel marketingu z użyciem mediów cyfrowych Digital Marketing Media oraz Creative dla wszystkich marek i produktów Kingston.

Tara Taubman-Bassirian
@clarinette02

Tarę można określić wieloma tytułami: prawniczka, adwokatka, mediatorka, badaczka, konsultantka, mówczyni i pisarka. Dzięki niesamowitej wiedzy specjalistycznej w takich obszarach, jak ochrona prywatności, własność intelektualna i ochrona danych, wyrobiła sobie pozycję w wielu krajach, w szczególności w Wielkiej Brytanii, Francji i Stanach Zjednoczonych.

Rafael Bloom
@rafibloom73

Rafael jest dyrektorem Salvatore Ltd. W tej roli pomaga firmom w zarządzaniu strategicznymi, komercyjnymi i proceduralnymi wyzwaniami i szansami wynikającymi ze zmian technologicznych i regulacyjnych.

Miriam Brown
@Kingston_MBrown

Menedżer ds. Marketingu strategicznego B2B w Kingston Technology i związana z firmą od 1997 roku. W swojej roli Miriam odpowiada za strategię marketingową, treść i kampanie dotyczące wszystkich produktów B2B firmy Kingston.

Sally Eaves
@sallyeaves

Prof. Sally Eaves była określana mianem "niosącej kaganek etycznej technologii". Ma głębokie doświadczenie na stanowiskach dyrektora naczelnego i dyrektora ds. technologii, jako profesor w dziedzinie nowych technologii oraz jako globalny doradca strategiczny. Sally Evans jest wielokrotnie nagradzaną międzynarodową prelegentką, autorką, badaczką i influencerką, dzielącą się oryginalnym i rzeczywistym przewodnictwem myślowym.

Ochrona danych i cyberbezpieczeństwo po wprowadzeniu RODO

Spis treści

Rozdział 1	Jak zmieniła się ochrona danych po wprowadzenia RODO?	5 – 7
Rozdział 2	Jak organizacje edukują swoich pracowników?	8 - 9
Rozdział 3	Czy działy IT mogą lepiej zabezpieczyć urządzenia?	10 - 11
Rozdział 4	Jak dostawcy technologii mogą ulepszyć procesy i zwiększyć ich zrozumienie?	12 - 13
	Podsumowanie	14
	o firmie Kingston	15

Rozdział 1 – Jak zmieniła się ochrona danych po wprowadzenia RODO?

Firmy przeszły długą drogę. W ciągu ostatnich dwóch lat zespoły prawne powiększyły się, a zatrudnienie inspektorów ochrony danych gwałtownie wzrosło[1] a konsultacje z zewnętrznymi doradcami ds. zachowania prywatności danych stały się bardziej popularne. Z przeprowadzaniem oceny wpływu na ochronę danych jest obecnie zaznajomione tysiące organizacji.

Jednak wciąż jest wiele do zrobienia.

Jednym z największych wyzwań związanych z RODO jest to, że trzeba być stale uważnym, ponieważ w większości organizacji prawie każdy członek personelu może w dowolnym momencie naruszać zasady. Problem nasila się w sektorach, w których pracownicy borykają się z nadmiarem obowiązków, posiadają duży stopień autonomii lub pracują zdalnie. Jest tak w dziedzinach takich jak opieka zdrowotna, edukacja i prawo. Dla przykładu wielu adwokatów nie myśli często o kwestiach poufności danych dotyczących prowadzonych spraw, wysyłając informacje w zwykłym załączniku do wiadomości e-mail. Pracownicy służby zdrowia będą wymieniać dane pacjentów lub np. wyniki skanowania rezonansu magnetycznego z niezabezpieczonych adresów e-mail. W organizacjach działających pod presją skrajnie wysokiego stresu wystarczy trochę dodatkowych zadań na liście rzeczy do zrobienia, aby zgodność z RODO przestała działać. Wydajność zwykle staje się ważniejsza niż procedury.

To musi ulec zmianie.

Istnieje jeszcze kwestia świadomości tego zagadnienia w sektorze charytatywnym. Zbyt często organizacje charytatywne wydają się uważać, że są zwolnione z RODO. Nawet jeśli zdają sobie sprawę z tego, że RODO ma zastosowanie do każdej organizacji prywatnej, publicznej i organizacji trzeciego sektora, często nie mają środków osobowych i finansowych na dostosowanie się do wymogów RODO.
Może to prowadzić do poważnych konsekwencji.Potencjalne kary, które grożą za naruszenie RODO są znacznie większe niż szacowane wydatki na IT.

Tara Taubman-Bassirian
@clarinette02

RODO, Konsultant ochrony danych i własności intelektualnej

„Wiele organizacji trzeciego sektora mówi:„ RODO nie dotyczy nas, jesteśmy tylko organizacją charytatywną ". Nawet w przypadku zgodności z RODO, nie chodzi o dane, które gromadzą, ale o to, że dopuszczają osoby trzecie do danych odwiedzających twoją stronę użytkowników. "

Od 2016 popyt na inspektorów ochrony danych gwałtownie wzrasta i zwiększył się o ponad 700%.

1. Varonis: A Year in the Life of the GDPR: Must-Know Stats and Takeaways www.varonis.com/blog/gdpr-effect-review/ [accessed 26.11.19]

Jak zmieniła się ochrona danych po wprowadzenia RODO?

Minimalizacja danych to zachęcający trend

Żyjemy w erze szybkiego i intensywnego gromadzenia danych. „Wielka Czwórka "The Big Four" (Google, Apple, Facebook i Amazon) przechowuje ogromne ilości danych klientów. Zakłada się, że inne organizacje mogą naśladować "Wielką Czwórkę" i gromadzić jak najwięcej danych. Jednakże im więcej danych posiadasz, tym na większe ryzyko się narażasz. Jednym z najbardziej pozytywnych trendów od czasu wprowadzenia RODO ograniczenie nadmiernego gromadzenia danych. Inteligentne firmy stosują więc etos określany mianem minimalizacji danych: jeśli ich nie potrzebujesz, nie zbieraj.

Tara Taubman-Bassirian
@clarinette02

RODO, Konsultant ochrony danych i własności intelektualnej

„Minimalizacja danych jest prawdopodobnie jednym z najlepszych pryncypiów będących efektem RODO. Każde utworzenie bazy danych oznacza ryzyko. "

Rob Allen
@Rob_A_kingston

Dyrektor ds. Marketingu i usług technicznych w Kingston Technology

„Mamy ścisłe zasady dotyczące usuwania danych. Tak, dane o znaczeniu krytycznym muszą być przechowywane we właściwy sposób. Ale w przypadku innych danych? Po roku ich już nie ma. Jaki jest sens, aby je trzymać? "

Korzyści wykraczają poza ograniczone ryzyko. Weźmy jako przykład marketing. Jeśli twoja marketingowa baza danych jest "niehigieniczna", być może przechowujesz nieaktualne dane. Gdy twoja baza danych obejmuje dziesiątki tysięcy osób i prowadzisz częste kampanie e-mail - marketingowe, koszty rosną. Wpływa to również na statystyki zaburzając skuteczność kampanii.

Minimalizacja danych dotyczy również danych składowanych w formie fizycznej, nie tylko cyfrowej. Uważaj na to, co drukujesz (np. skany paszportów klientów); uważaj, co zapisujesz (np. hasła do konta). A kiedy musisz zachować fizyczną kopię czegoś, przechowuj ją bezpiecznie. Ta góra dokumentów na biurku może wyglądać imponująco, ale z pewnością nie jest szczytem bezpieczeństwa.

Rafael Bloom
@rafibloom73

Dyrektor,
Salvatore Ltd

„To, czego jesteśmy świadkami jest zupełnie innym sposobem myślenia o interfejsie między technologią, a rzeczywistą działalnością firmy. Taki poziom dojrzałości cyfrowej wśród liderów biznesu bezwzględnie musiał się pojawić."

Wpływ narażenia: od dyrektorów do konsumenta

Ochrona danych jako koncepcja regulacyjna istnieje od dziesięcioleci. Jednak wysokie grzywny nałożone dotychczas na takie firmy, jak Google[1], British Airways i sieć hoteli Marriott[2] oraz popularność tego tematu w mediach przyniosły tematyce związanej z RODO uwagę najwyżej postawionych osób w firmach. To natomiast wywołało tzw. efekt spływania w dół.

1. Varonis: A Year in the Life of the GDPR: Must-Know Stats and Takeaways www.varonis.com/blog/gdpr-effect-review/ [accessed 26.11.19]
2. The Guardian: GDPR fines: where will BA and Marriott's £300m go? www.theguardian.com/business/2019/jul/10/gdpr-fines-ba-british-airways-marriott-data-watchdog [accessed 26.11.19]

Jak zmieniła się ochrona danych po wprowadzenia RODO?

Kontynuacja...

Inną siłą napędową przyjęcia mocnej ochrony danych jest współpraca biznesowa. Duże firmy dokładają teraz wzmożonej staranności w zakresie integralności bezpieczeństwa danych potencjalnego dostawcy, ponieważ nie chcą ponosić odpowiedzialności za naruszenia danych przez współpracowników.

Istnieje również druga strona medalu zwiększonej świadomości na temat RODO: konsumenci są bardziej świadomi swoich praw do danych. Wiedzą też, że jeśli firma traci kontrolę nad przechowywanymi przez nią danymi - uwaga: niekoniecznie nawet w wyniku włamania - mają prawo do odszkodowania. Firmy muszą pozostawać skoncentrowane na zapewnieniu bezpieczeństwa.

Sally Eaves
@sallyeaves

CEO i Dyrector,
Sally Eaves Consultancy

"Ochrona danych stała się imperatywem w biznesie, dzięki niej zdobywa się lub traci zaufanie"

Rozdział 2 – Jak organizacje edukują swoich pracowników?

Szkolenie personelu: dwa słowa zdolne do wywołania znużenia wśród pracowników.

To jeszcze jeden powódó, aby upewnić się, że twoje szkolenie jest angażujące. Odpowiednio wyedukowani pracownicy rzadziej naruszają dobre praktyki w zakresie ochrony danych. A jeśli dojdzie do naruszenia danych, Biuro Komisarza ds. Informacji (ICO – odpowiednik UODO) będzie bardziej przychylne, jeśli udowodnisz, że podjąłeś wszelkie możliwe działania w celu przeszkolenia personelu w zakresie bezpieczeństwa danych.

Rafael Bloom
@rafibloom73

Director,
Salvatore

„Lubię myśleć o danych jako o elemencie łańcucha dostaw, w przypadku którego ich pochodzenie i cały cykl życia wymagają odpowiedniego zarządzania. To oczywiście dobrze; zebrać swój zespół w jednym pomieszczeniu na pół godziny i opowiedzieć im co robić, prosić by nie niszczyli wydruków oraz by mieli w miarę przyzwoite hasło. Jasne, właśnie zmniejszyłeś ryzyko dla organizacji. Ale ostatecznie, tak naprawdę, czy istnieje istotna różnica oprócz początkowego niewielkiego wpływu, który narzuciłeś na ludzi? Nie."

Jednak w kwietniu 2019 r. Minister ds. cyfrowych Wielkiej Brytanii, Margot James zasugerowała, że trzy na dziesięć brytyjskich organizacji przeszkoliło pracowników w zakresie radzenia sobie z zagrożeniami cybernetycznymi[1]. Czas poważnie potraktować szkolenia.

Chodzi o tworzenie kultury, a nie szkolenie z zaznaczania pól wyboru

W szkoleniu chodzi o uzyskanie rzeczywistego wpływu na zmianę zachowań i kultury pracy, a nie wypełnianie pól w formularzach. Łatwo jest kupić pakiet szkoleniowy online z kilkoma prostymi pytaniami na temat ochrony danych, na które każdy może odpowiedzieć poprawnie. Ale czy to naprawdę pomoże chronić Twoją organizację?

Dobre zachowania w zakresie ochrony danych mają dwa podstawowe czynniki. Po pierwsze, szkolenie, które jest inteligentne, angażujące i ukierunkowane na unikalne wyzwania Twojej organizacji. Po drugie, uświadomienie sobie, że RODO jest dogłębnie związane z kulturą miejsca pracy, która codziennie wpływa na wszystkich pracowników. Chodzi o właściwe traktowanie danych w całej organizacji. Weźmy na przykład HR. Pomyśl o wszystkich danych osobowych kandydatów, które znajdują się na serwerach e-mail.
Ochrona danych to wspólna odpowiedzialność

1. Intelligent CISO: One year on, what has been the impact of GDPR on data security? www.intelligentciso.com/2019/04/16/one-year-on-what-has-been-the-impact-of-gdpr-on-data-security/ [accessed 26.11.19]

Jak organizacje edukują swoich pracowników?

Za danymi kryje się człowiek

W pierwszej części zwróciliśmy uwagę na fakt, że konsumenci stają się bardziej świadomi swoich praw do danych. Dobrym sposobem na szkolenie w zakresie ochrony danych jest uświadomienie pracownikom , że za danymi zawsze stoi jakaś osoba. Poproś swoich pracowników, aby pomyśleli o każdej organizacji, której przekazali własne dane, a zdadzą sobie sprawę, że w ochronie danych chodzi głównie o prywatność osób.

Miej plan awaryjny

Sally Eaves
@sallyeaves

„Ciągłe szkolenie pracowników na temat bezpieczeństwa danych i prywatności jest koniecznością biznesową. Nie może to być jednorazowa, prowadzona raz w roku sesja szkoleniowa, ale raczej proaktywne, interaktywne i angażujące doświadczenie, będące częścią codziennej pracy. Pracownicy muszą brać udział w dialogu na temat tego, co chcemy ograniczać, zarządzać i czego bronić. "

Miriam Brown
@Kingston_MBrown

„Myślę, że to, co jest interesujące podczas szkolenia, to gdy mówisz do ludzi - a gdyby to były twoje dane? - Gdyby menedżer mojego banku pracował z domu na swoim laptopie i miał na nim wrażliwe informacje, chciałbym, żeby znajdowały się na zaszyfrowanym nośniku. "

Rob Allen
@Rob_A_kingston

"Traktuj dane tak, jakby były twoimi"

Rozdział 3 – Czy działy IT mogą lepiej zabezpieczyć urządzenia?

Praca zdalna stała się naszą codziennością

Twoi pracownicy prawdopodobnie uzyskują dostęp do środowiska pracy z kilku różnych urządzeń - w tym urządzeń osobistych, które są łatwo zostawić w pociągu lub zgubić w taksówce. Twoim wyzwaniem jest znalezienie sposobu, aby pomóc swoim pracownikom w wydajnej pracy bez narażania się na zagrożenia bezpieczeństwa i włamania. Wystarczy błąd jednej osoby, aby zniweczyć Twoje działania związane z ochroną danych.

Sally Eaves
@sallyeaves

CEO i dyrektor,
Sally Eaves Consultancy

„Dane muszą być chronione podczas przesyłania, przechowywania i podczas użytkowania - bardzo ważne jest, aby mieć wszechstronny plan bezpieczeństwa, odzyskiwania i usuwania danych, obejmujący wszystkie te konteksty. Szczególnie ważne jest zwrócenie uwagi na obszary ryzyka, które są często niedoceniane. Za przykład mogą służyć niezaszyfrowane pamięci USB, korzystanie z poczty e-mail do wysyłania niezaszyfrowanych załączników oraz funkcje przeglądarki internetowej ujawniające wrażliwe dane użytkownika. Przy tak wielu podłączonych urządzeniach i ewoluujących wzorcach pracy, niezwykle ważne jest, aby dane przechowywane w telefonie komórkowym były równie bezpieczne, jak dane przechowywane na serwerze firmowym. "

Logowanie dwuskładnikowe

Dla przeciętnej organizacji zdecydowanie najlepszą i najłatwiejszą rzeczą, jaką może zrobić, jest ochrona tzw. sieci granicznej - i to naprawdę może być tak proste, jak stosowanie menedżerów haseł i uwierzytelnianie dwuskładnikowe. Dobrym przykładem uwierzytelniania dwuskładnikowego jest monitowanie użytkownika o podanie hasła na laptopie oraz kodu, który jest wysyłany na telefon komórkowy po pomyślnym podaniu hasła.

VPNy i szyfrowane SSD/USB

Sieci VPN są coraz bardziej popularne wśród małych i średnich przedsiębiorstw. Są szczególnie istotne dla pracowników, którzy uzyskują dostęp do danych biznesowych za pośrednictwem publicznych sieci WIFI. Jednakże firmy muszą uważać, aby nie przeceniać możliwości VPNów. Są częścią rozwiązania, a nie jego całością. Zbyt często firmy wdrażają sieci VPN, aby zdalni pracownicy mogli używać laptopów bez szyfrowania sprzętowego. Prawie wszyscy przechowują pliki na swoim laptopie. Co się stanie, jeśli urządzenie zostanie zaatakowane przez hakera, zgubione lub skradzione? Zaszyfrowane nośniki USB i SSD są tylko nieznacznie droższe niż ich standardowe wersje. Wdrażanie zaszyfrowanych urządzeń USB i wyposażanie notebooków w sprzętowo szyfrowane dyski SSD to długa, mozolna droga do rozwiązania problemów związanych z pracą zdalną. A jeśli urządzenie zostanie zgubione lub skradzione, możesz mieć pewność, że nikt nie będzie miał dostępu do zaszyfrowanych plików. Możesz nawet zdalnie zniszczyć utracone nośniki USB.

„Kiedyś było mi dane poznać eksperta ds. cyberbezpieczeństwa, który próbował przekonać dyrektora generalnego firmy do przyjęcia uwierzytelniania dwuskładnikowego, ale spotkał się z oporem: „Nie, nie robimy tego, to uciążliwe, to dodatkowy krok, ja tego nie chcę." Wkrótce potem padli ofiarą oszustwa w wysokości 40 000 £."

Rafael Bloom
@rafibloom73

Director, Salvatore Ltd

„Ostatecznie najlepszym sposobem na zwiększenie świadomości bezpieczeństwa jest otwarte rozmawianie z pracownikami w celu znalezienia strategii, które są zarówno bezpieczne, jak i produktywne."

Rob Allen
@Rob_A_kingston

Dyrektor marketingu i usług technicznych, Kingston Technology

Czy działy IT mogą lepiej zabezpieczyć urządzenia?

Własne serwert i MSP

Coraz większa liczba dużych organizacji robi krok w kierunku posiadania własnych serwerów, zlokalizowanych we własnej serwerowni. Oznacza to, że mają one pełną kontrolę nad swoimi serwerami, a nic nie jest przechowywane w publicznie dostępnej chmurze. Są też hybrydowe rozwiązania serwerowe, w których mniej wrażliwe dane pozostają w chmurze, ale dane osobowe pozostają na własnym serwerze. Dla małych i średnich firm i organizacji z trzeciego sektora posiadanie własnego serwera może być zbyt kosztowne. I tu właśnie wkraczają usługi MSP i wirtualne prywatne serwery (VPS). Zwiększa to bezpieczeństwo, bez dużego zwiększania kosztów operacyjnych.

Automatyczne oznaczanie wygasających danych

Jednym z założeń RODO jest konieczność usuwania starych danych. Na przykład niektóre rodzaje danych osobowych nie mogą być przechowywane dłużej niż siedem lat. A co, jeśli zostaniesz automatycznie zapytany, kiedy dane wkrótce „wygasną"? Dzięki odpowiedniej bazie danych Twojemu zespołowi IT będzie łatwiej stworzyć akcję, która wysłałaby automatycznie wygenerowany e-mail do inspektora ochrony danych, gdy zbliżać się będzie kres utrzymywania konkretnych danych.

Praca z właściwymi producentami

Jeśli chodzi o bezpieczeństwo IT, istnieje niezliczona liczba producentów i sprzedawców. Rozeznaj rynek. Chodzi przede wszystkim o posiadanie systemu pochodzącego od zaufanego dostawcy posiadającego specjalistyczną wiedzę w zakresie wspierania organizacji w Twojej branży lub sektorze. Upewnij się, że wybrani dostawcy nie tylko dysponują technologią, ale także rozumieją wyzwania związane z wdrożeniem, jeśli chodzi o bezpieczeństwo danych.

Rozdział 4 – Jak dostawcy technologii mogą ulepszyć procesy i zwiększyć ich zrozumienie?

TLC dla inspektora ochrony danych osobowych

Od 2016 r. zapotrzebowanie na inspektorów ochrony danych gwałtownie wzrósło, a ich liczaę zwiększyła się o ponad 700%.[1] Obecnie w całej Europie zatrudnionych jest ponad 500 000 inspektorów ochrony danych - to sześć razy więcej niż przewidywano w 2017 r.[2] A jednak znaczenie roli inspektora ochrony danych jest często pomijane i trywializowane.

Inspektor ochrony danych (IOD) wymaga pełnego wglądu w polityki bezpieczeństwa i prywatności Twojej firmy. To praca na pełen etat. Jednak w niektórych organizacjach "IOD" to po prostu etykieta przypisana komuś z regularnego personelu, który najlepiej rozumie technologię. Są odpowiedzialni za prywatność danych w całej firmie, a jednocześnie wykonują swoje codzienne obowiązki.

Rzeczywistość jest taka, że musi istnieć szereg profesjonalnych usług i narzędzi, aby wspierać tę nową klasę IOD. Nawet jeśli masz pełnoetatowego inspektora ochrony danych, zagadnienia z zakresu bezpieczeństwa danych zmieniają się szybko i zawsze pojawią się wyzwania wymagające dodatkowej opinii ekspertów. Współpraca z zewnętrzną firmą doradczą lub doradcą ds. bezpieczeństwa danych może okazać się konieczna na dłuższą metę, ale najpierw musisz stworzyć odpowiedni szkic tego, jak ma wyglądać bezpieczeństwo danych opracowany wewnętrznie tak dokładnie, jak to możliwe.

Przejrzystość, elastyczność i spójność

Twoja infrastruktura IT jest tak silna, jak jej najsłabszy element. Dlatego w przypadku każdego nowego dodatku do infrastruktury IT dostawca technologii powinien zapewnić pełną informację na temat potencjalnych zagrożeń bezpieczeństwa i udzielić odpowiednich porad dotyczących bezpiecznego korzystania z nowego produktu.

Tara Taubman-Bassirian
@clarinette02

RODO, Ochrona danych i konsultant własności intelektualnej

„Staram się tłumaczyć osobom, które instalują kamery do monitoringu wszędzie, że niekoniecznie są to realne zabezpieczenia, ponieważ często są instalowane bez hasła. Możesz więc zalogować się na stronie internetowej, usiąść i obserwować obraz z tych kamer. W rzeczywistości mówi się w ten sposób złodziejowi: „Przyjdź i sprawdź, kiedy mnie tam nie ma!"

1. Varonis: A Year in the Life of the GDPR: Must-Know Stats and Takeaways www.varonis.com/blog/gdpr-effect-review/ [accessed 26.11.19]
2. The Guardian: GDPR fines: where will BA and Marriott's £300m go? www.theguardian.com/business/2019/jul/10/gdpr-fines-ba-british-airways-marriott-data-watchdog [accessed 26.11.19]

Jak dostawcy technologii mogą ulepszyć procesy i zwiększyć ich zrozumienie?

Istnieje problem elastyczności. Co się stanie, gdy produkt osiągnie koniec okresu użytkowania lub będzie wymagał aktualizacji? Dostawcy technologii powinni udzielać porad na temat postępowania na wypadek awarii swoich produktów i niezamierzonego narażenia na szwank posiadanych danych lub bezpieczeństwa infrastruktury IT. Weźmy na przykład skaner MRI. Może być wyposażony w czteroterabajtowy szyfrowany dysk SSD do przechowywania zdjęć pacjentów. Ale co się stanie, gdy skończy się ta pamięć?

Dostawcy technologii i same organizacje muszą również ułatwiać budowę środowiska spójności cyfrowej i spójności danych - zarówno w organizacji, jak i podczas współpracy z zewnętrznymi dostawcami i partnerami. Jest to szczególnie ważne w przypadku wieloaspektowych, wielooddziałowych i wielozakresowych organizacji, takich jak NHS (National Health Service - służba zdrowia w Wielkiej Brytanii).

Miriam Brown
@Kingston_MBrown

B2B Strategic Marketing Manager w Kingston Technology

„Sprzedaliśmy wiele produktów do NHS - ale istnieją wyraźne różnice między poszczególnymi funduszami, gdy pytamy, jakie mają zasady i protokoły ochrony danych".

Analiza Horizon-scanning

Technologia zmienia się niezwykle szybko, czasem wyprzedzając bezpieczeństwo. W przypadku pojawiających się technologii - takich jak płatność za pomocą rozpoznawania twarzy w Chinach - czasami zdarza się, że organizacje starają się wprowadzić tę technologię, zanim przemyślą dokładnie potencjalne konsekwencje dla bezpieczeństwa i ochrony danych. Powszechna dostępność sieci 5G stanie się faktem już za rok lub dwa, a edge computing i rozproszone centra danych staną się rzeczywistością. Dostawcy technologii muszą być w stanie pomóc organizacjom w bezpiecznym korzystaniu z powstających technologii bez narażania własnej integralności danych lub bezpieczeństwa IT.

Sally Eaves
@sallyeaves

CEO i dyrektor, Sally Eaves Consultancy

„Wierzę, że zaczniemy widzieć zmianę w RODO, polegającą na zmniejszeniu problemów związanych z wdrażaniem, a skupieniu się na optymalizacji korzyści, takich jak ulepszone procesy informatyczne, tworzenie backupów i odzyskiwanie danych oraz poprawione bezpieczeństwo, i wykorzystywanie ich jako przewagi konkurencyjnej względem innych podmiotów z branży. "

Podsumowanie

RODO zmieniło biznes na lepsze, zwracając uwagę na prywatność danych i bezpieczeństwo sieci zarówno wśród kadry dyrektorskiej, jak i klientów. Zgodność z rozporządzeniem wymaga jednak ciągłej dbałości o bezpieczeństwo danych - każdego dnia – przez każdego pracownika. Ciągle ewoluujący charakter technologii i cyberzagrożeń oznacza, że dobra infrastruktura bezpieczeństwa i dobre szkolenie - poparte właściwym doradztwem w zakresie technologii i prywatności danych - mają kluczowe znaczenie dla biznesu. Przypominanie pracownikom, że za danymi zawsze stoi człowiek, może znacznie przyczynić się do upowszechnienia ochrony danych w kulturze pracy. Zmiana kulturowa jest o wiele bardziej skuteczna niż jakiekolwiek szkolenie.

o firmie Kingston

Dzięki 32-letniemu doświadczeniu firma Kingston ma wiedzę pozwalającą na identyfikację i rozwiązywanie problemów związanych z pracą zdalną - ułatwiając pracownikom bezpieczną pracę z dowolnego miejsca, bez narażania organizacji.

#KingstonIsWithYou