
Kingston
TECHNOLOGY
Wyzwania związane z bezpieczeństwem pracy zdalnej oraz sposoby, jak im sprostać
#KingstonIsWithYou

Wyzwania związane z bezpieczeństwem pracy zdalnej oraz sposoby, jak im sprostać

Wstęp

Najwyższy czas, aby pracownicy naprawdę zaczęli dbać o bezpieczeństwo danych. Wiadomo już, że praca zdalna leży u podstaw działalności wielu firm. Jednak nie można ignorować zagrożeń dotyczących bezpieczeństwa sieci oraz zgodności z rozporządzeniem o ochronie danych osobowych (RODO). Wiele firm sądzi, że utrzymanie jakościowej kontroli nad środowiskiem IT to wyzwanie, któremu nie można sprostać bez ponoszenia wysokich kosztów. Nie musi tak jednak być, a koszty nie mogą być wymówką.

Na rynku dostępne są różne systemy, usługi oraz produkty, których implementacja nie zawsze wiąże się z wysokim kosztem. W praktyce wyzwania związane z bezpieczeństwem nie dotyczą tylko finansów, czy technologii, ale też kultury organizacyjnej przedsiębiorstwa. Względnie łatwo można stworzyć środowisko IT do pracy zdalnej, jeśli jednak pracownicy nie będą postępować zgodnie z procedurami bezpieczeństwa danych oraz obwiązującymi regulacjami, firma będzie borykać się z trudnościami. A potencjalne koszty naruszeń bezpieczeństwa danych są niezwykle wysokie.

Na rynku dostępne są odpowiednie produkty, jednak podstawę stanowi edukacja pracowników.

Nasi eksperci

Ten krótki e-book został opracowany przez troje specjalistów ekspertów w dziedzinie bezpieczeństwa danych oraz pracy zdalnej.

Rob Allen
@Rob_A_kingston

Rob Allen jest dyrektorem działu marketingu i usług technicznych w Kingston Technology. Pracuje w firmie od 1996 roku. Jest odpowiedzialny za pracę działów PR, mediów społecznościowych, channel marketingu oraz digital marketingu.

Rafael Bloom
@rafibloom73

Rafael Bloom jest dyrektorem firmy Salvatore ltd, która pomaga przedsiębiorstwom zarządzać strategicznymi, handlowymi oraz proceduralnymi wyzwaniami, które są wynikiem zmian technologicznych i prawnych.

Sarah Janes
@SarahkJanes

Sarah Janes jest od 2014 roku dyrektorem zarządzającym firmy Layer 8 Ltd. Jej misją jest wspieranie managerów ds. bezpieczeństwa danych w skutecznym zarządzaniu zmianami dotyczącymi kontroli bezpieczeństwa sieci w różnej wielkości przedsiębiorstwach.

Wyzwania związane z bezpieczeństwem pracy zdalnej oraz sposoby, jak im sprostać

Spis treści

Część 1. Problem - pracownicy a praca zdalna

Kluczowe znaczenie dostępu zdalnego

Już dawno minęły czasy, gdy praca mogła być wykonywana tylko w siedzibie firmy. Dzisiaj pracownicy sprawdzają pocztę e-mail na swoich prywatnych smartfonach, dyrektor operacyjny całymi dniami pracuje z domu lub z ulubionej kawiarni, a handlowcy łączą się z firmową siecią z siedziby klientów. Praca zdalna jest nowym standardem.

Dzięki niej wzrasta produktywność i zmniejsza się rotacja personelu,[1] maleją koszty firmy,[2] zmniejsza się zanieczyszczenie środowiska.[3] Badania wykazują, że **70% specjalistów pracuje zdalnie co najmniej raz w tygodniu.**[4]

Jednak jedna osoba może narazić integralność całej organizacji, jeśli nie będzie stosować się do obowiązujących protokołów bezpieczeństwa.

Zgodność procedur z rozporządzeniem RODO stanowi konieczność

Zastosowanie odpowiednich środków bezpieczeństwa nie powinno podlegać dyskusji, zarówno ze względu na bezpieczeństwo firmy, jak i wymóg zapewnienia zgodności z rozporządzeniem RODO, którego nie można lekceważyć. Brytyjskie Biuro ds. danych osobowych (Information Commissioner's Office, ICO) niedawno nałożyło grzywnę na firmy British Airways oraz na sieć hoteli Marriot o łącznej wysokości 300 milionów funtów za naruszenie przepisów ochrony danych osobowych.[5]

70% specjalistów pracuje zdalnie co najmniej raz w tygodniu.[4]

Jakie organizacje są narażone na ryzyko?

Na ryzyko narażone są organizacje, których pracownicy wykonują pracę zdalnie lub korzystają z prywatnych urządzeń w celu podłączenia się do sieci firmowej. Taki nasuwa się wniosek.

[1] **Inc.com: A 2-Year Stanford Study Shows the Astonishing Productivity Boost of Working From Home -** www.inc.com/scott-mautz/a-2-year-stanford-study-shows-astonishing-productivity-boost-of-working-from-home.html

[2] **PGi: What are the cost savings of telecommuting? -** www.pgi.com/blog/2013/03/what-are-the-cost-savings-of-telecommuting/

[3] **FlexJobs: 5 stats about telecommuting's environmental impact -** www.flexjobs.com/blog/post/telecommuting-sustainability-how-telecommuting-is-a-green-job/

[4] **CNBC: 70% of people globally work remotely at least once a week, study says -** www.cnbc.com/2018/05/30/70-percent-of-people-globally-work-remotely-at-least-once-a-week-iwg-study.html

[5] **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

Część 2. Dostęp zdalny - wyzwania

Praca zdalna niesie ze sobą szereg wyzwań związanych z bezpieczeństwem.

Mogą być trudne do rozwiązania, jednak potrzeba zapewnienia integralności firmy wymusza ich poważne traktowanie.

Sarah Janes
@SarahkJanes

Dyrektor zarządzająca Layer 8 Ltd

„Największa obawa związana z RODO dotyczy kontroli organizacji nad przetwarzaniem przez nią danych osobowych. Jest ona niemożliwa, jeżeli firma nie wie, w jaki sposób są one przechowywane".

Firmom nie jest łatwo dostosować systemy i urządzenia do tempa, w jakim rozwija się technologia.

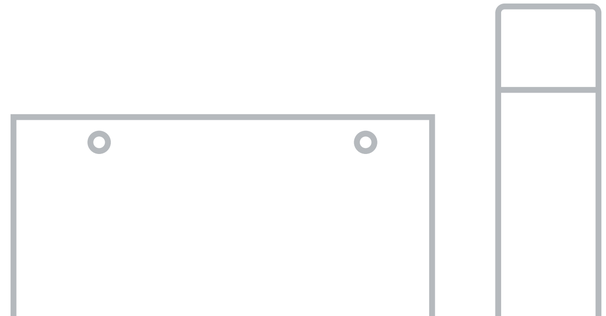
38% osób pracujących zdalnie dla małych i średnich przedsiębiorstw uważa, że nie ma wsparcia technologicznego ani wiedzy, które mogą pomóc im w pracy zdalnej z domu lub z miejsc publicznych.

W rezultacie, pracownicy mogą poszukiwać dróg obejścia problemów, co wiąże się z prawdopodobieństwem negatywnego wpływu na procedury ochrony danych oraz uczynieniem organizacji podatnej na zagrożenia związane z bezpieczeństwem. Procedury bezpieczeństwa muszą umożliwiać pracownikom skuteczne działanie, w przeciwnym razie będą szukali nieautoryzowanych rozwiązań, umożliwiających przechowywanie danych w miejscach takich jak Slack, Dropbox, osobista poczta e-mail lub prywatne nośniki USB. Dodatkowo, pomiędzy działem IT, a pracownikiem może zrodzić się kultura wrogości (przeciwstawienie My – Oni), prowadząca do narażenia firmy na ryzyko.

Rob Allen
@Rob_A_kingston

Dyrektor ds. marketingu i usług technicznych w firmie Kingston Technology

„Z mojego doświadczenia wynika, że im większa firma, tym większe mogą być ograniczenia i niedogodności dla pracowników zdalnych, związane ze zbyt długim czasem logowania do systemu oraz koniecznością dostosowania się do wymaganych zabezpieczeń".



Część 2. Dostęp zdalny - wyzwania

Pracuj ze swojego urządzenia (BYOD)

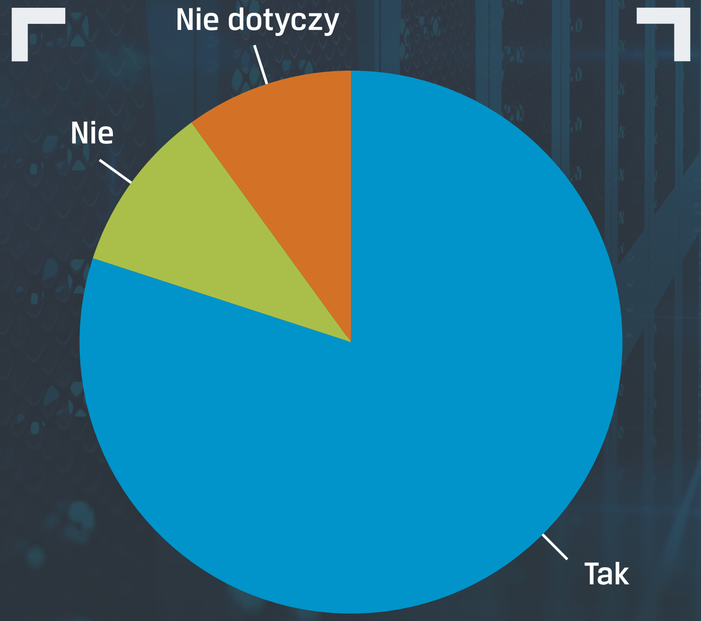
Współcześni specjaliści często sprawdzają służbową pocztę e-mail na własnych smartfonach, a także mają dostęp do danych firmy z prywatnych laptopów i tabletów, co stanowi potencjalne źródło zagrożenia bezpieczeństwa organizacji. Czy Twój zespół przesyła dane poza firmę? Czy jego sprzęt jest odpowiednio skonfigurowany i wyposażony w zabezpieczające oprogramowanie? Trzeba szczerze odpowiedzieć sobie na te pytania.

Sarah Janes
@SarahkJanes

Dyrektor zarządzająca
Layer 8 Ltd

„Duże wyzwanie stanowi zrozumienie, gdzie przechowywane są dane organizacji".

Czy obawiasz się, że pracownicy znajdą sposoby na obejście obowiązujących środków bezpieczeństwa?



Źródło: Ankieta firmy Kingston, 2019 r.

Publiczne sieci Wi-Fi

Potencjalne zagrożenia dotyczą nie tylko pracy z domu. Logowanie się do sieci firmowej z kawiarni z filiżanką kawy w ręku? Publiczne sieci Wi-Fi to raj dla hakerów a pracownicy powinni być uzbrojeni w wiedzę i odpowiednie zabezpieczenia, by ograniczyć każde potencjalne ryzyko.

Cyberataki i zaawansowany phishing

Phishing, czyli oszustwo skierowane do wybranych pracowników, staje się coraz bardziej wyrafinowane i przekonujące. Czy Twoi pracownicy są odpowiednio przeszkoleni, by rozpoznać to zagrożenie oraz stale ewoluujące oprogramowania malware i ransomware? Wszystkie urządzenia należące do organizacji muszą być zabezpieczone.

Część 3. Infrastruktura dostępu zdalnego (oraz uwagi na temat świadomości istnienia problemu bezpieczeństwa danych)

Istnieją technologie, które mogą uprościć wyzwania związane z właściwym zabezpieczeniem pracy zdalnej. I nie są to technologie bardzo kosztowne.

Projektowanie odpowiedniej infrastruktury

Pracodawcy muszą mieć pewność, że pracownicy zdalni mogą w łatwy i skuteczny sposób uzyskać dostęp do odpowiednich narzędzi i danych, by produktywnie wykonywać codzienne zadania. Nie musi się to jednak wiązać z wprowadzaniem nowych produktów, ale przede wszystkim z wyborem właściwej infrastruktury. Dla przykładu, w większości firm potrzebne są komputery lub laptopy, należy więc wybrać szyfrowane dyski twarde lub SSD. Dzięki temu w przypadku utraty lub kradzieży urządzenia, dane firmy będą zabezpieczone przed dostaniem się w niepowołane ręce. Dodatkowo, w przypadku naruszenia danych biuro UODO potraktuje firmę przychylniej wiedząc, że podjęła środki mające na celu zabezpieczenie danych.

Praca z właściwymi dostawcami

W branży bezpieczeństwa IT działa wielu producentów i dostawców. Należy więc upewnić się, że system pochodzi od zaufanego dostawcy, posiadającego odpowiednią wiedzę w zakresie rozwiązań do pracy zdalnej.

Sieci VPN

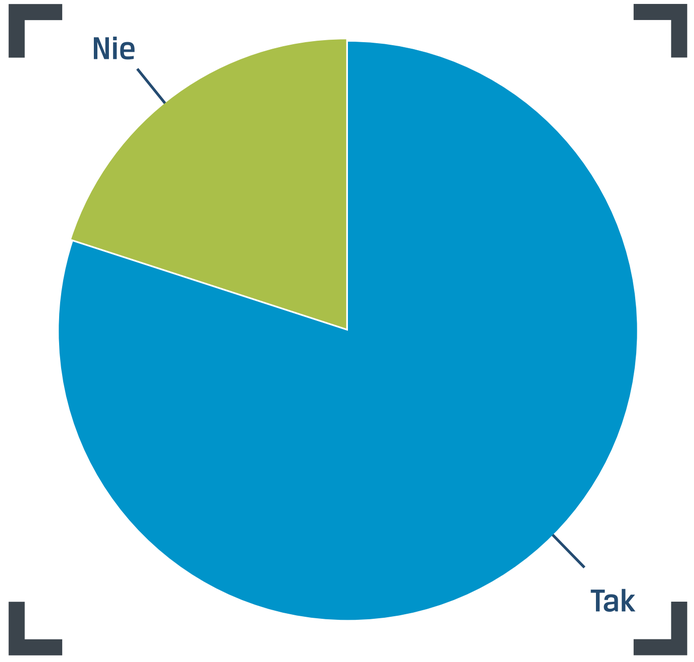
Jeżeli do zabezpieczenia organizacji konieczne jest korzystanie z sieci VPN, udostępnienie odpowiednich narzędzi właściwym osobom znacząco ogranicza ryzyko. Sieci VPN są szczególnie istotne dla pracowników, którzy mają dostęp do danych firmy i korzystają z publicznych sieci Wi-Fi.

Programy do ochrony danych (DLP)

Praktycznie wszystkie programy do ochrony danych (DLP) umożliwiają ograniczenie dostępu do sieci, jednocześnie zezwalając na dostęp określonych urządzeń, takich jak szyfrowane pamięci USB, które zaprojektowano tak, by były jednoznacznie identyfikowalne. Wiąże się to z minimalnym kosztem. (Warto zapoznać się z szeroką ofertą pamięci szyfrowanych USB firmy Kingston, które można spersonalizować do potrzeb organizacji).

Czy konieczne jest/było wprowadzenie istotnych zmian, by zapewnić zgodność firmy z wymogami rozporządzenia RODO?

Źródło: Ankieta firmy Kingston, 2019 r.



Część 3. Infrastruktura dostępu zdalnego (oraz uwagi na temat świadomości istnienia problemu bezpieczeństwa danych)

Pamięci USB i nośniki SSD

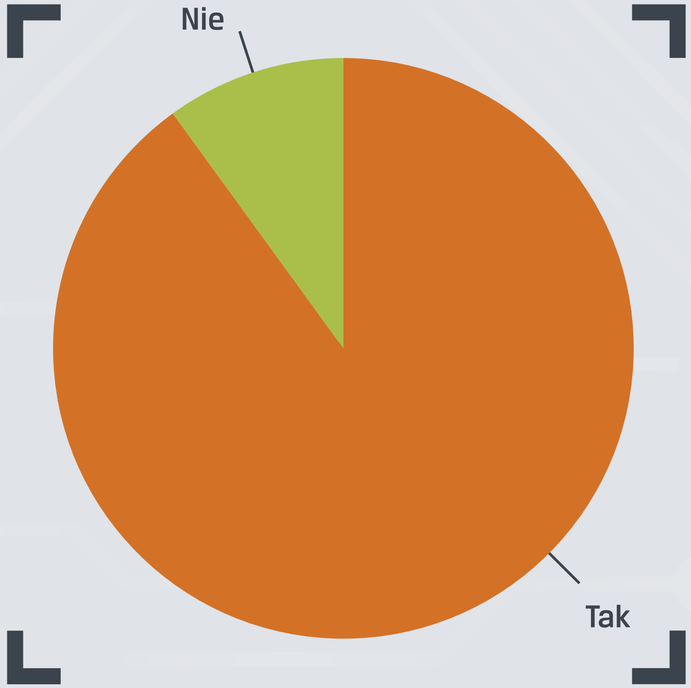
Wdrażanie szyfrowanych pamięci USB oraz wyposażenie notebooków w szyfrowane nośniki SSD to duży krok w kierunku sprostania wyzwaniom związanym z pracą zdalną. Dzięki stosowaniu szyfrowanych pamięci USB i sprzętowo szyfrowanych nośników SSD dane są zabezpieczone w każdym miejscu i w każdej chwili (niezależnie od połączenia z siecią Wi-Fi). W przypadku utraty lub kradzieży urządzenia można mieć pewność, że nikt nie uzyska dostępu do zaszyfrowanych plików. W niektórych przypadkach istnieje również możliwość zdalnego zniszczenia danych na pamięci USB.

Zawsze bądź przygotowany na najgorszy scenariusz

Czasem zbyt optymistyczne podejście przeradza się w ślepą wiarę w technologię. Zespół ds. bezpieczeństwa zawsze powinien zakładać negatywną dla organizacji wersję wydarzeń. Mimo zaufania wobec pracowników i środkom bezpieczeństwa, należy brać pod uwagę najgorszy scenariusz. Na spójność zabezpieczeń sieci firmy doskonale wpływa założenie, że mogą one zostać złamane.

Czy system zabezpieczania punktów końcowych organizacji obejmuje urządzenia mobilne pracowników, takie jak pamięci USB, notebooki itp.?

Źródło: Ankieta firmy Kingston, 2019 r.



Część 4. Edukacja pracowników to konieczność

Odpowiednia technologia to zaledwie połowa sukcesu. Prawdziwe problemy pojawiają się, gdy pracownicy są pozostawieni bez nadzoru. Dlatego kwestia bezpieczeństwa dotyczy zarówno kultury miejsca pracy, jak i technologii. Bez odpowiedniej edukacji pracownicy będą postrzegać rozporządzenie RODO, dyrektywę o prywatności i łączności elektronicznej (PECR) oraz inne panujące reguły tylko jako uciążliwość.

Jak temu zaradzić?

Uzasadnij wszystkie wprowadzane zasady

„Nie idź za tamto drzewo".
„Nie idź za tamto drzewo, bo tam jest lew".

Które zdanie jest łatwiej zapamiętać? Ludzie chętniej przestrzegają obowiązujących zasad, gdy znają ich uzasadnienie. Pomóż swoim pracownikom zrozumieć, dlaczego je wprowadzono.

Odnieś się do osobistych doświadczeń pracowników

Pracownicy lepiej zrozumieją zagrożenia, gdy odniosą je do swoich doświadczeń. Weźmy na przykład rozporządzenie RODO. Aby pomóc zespołowi zrozumieć, że za każdym zbiorem danych kryje się osoba, warto ich zapytać, jakby się czuli, gdyby organizacja przechowująca ich dane miała do tego bardzo niedbałe podejście. Jakby się czuli, gdyby ich dane dostały się w niepowołane ręce?

„Jeśli wyjaśni się pracownikom, że bezpieczeństwo i przestrzeganie RODO leży w ich własnym interesie także poza życiem zawodowym, łatwiej zrozumieją, dlaczego firma jest zobowiązana chronić dane".

Rafael Bloom
@rafibloom73
Dyrektor firmy Salvatore Ltd

„Ostatecznie najlepszym sposobem zwiększenia świadomości na temat cyberbezpieczeństwa są rozmowy z pracownikami, na podstawie których można opracować odpowiednie strategie bezpieczeństwa".

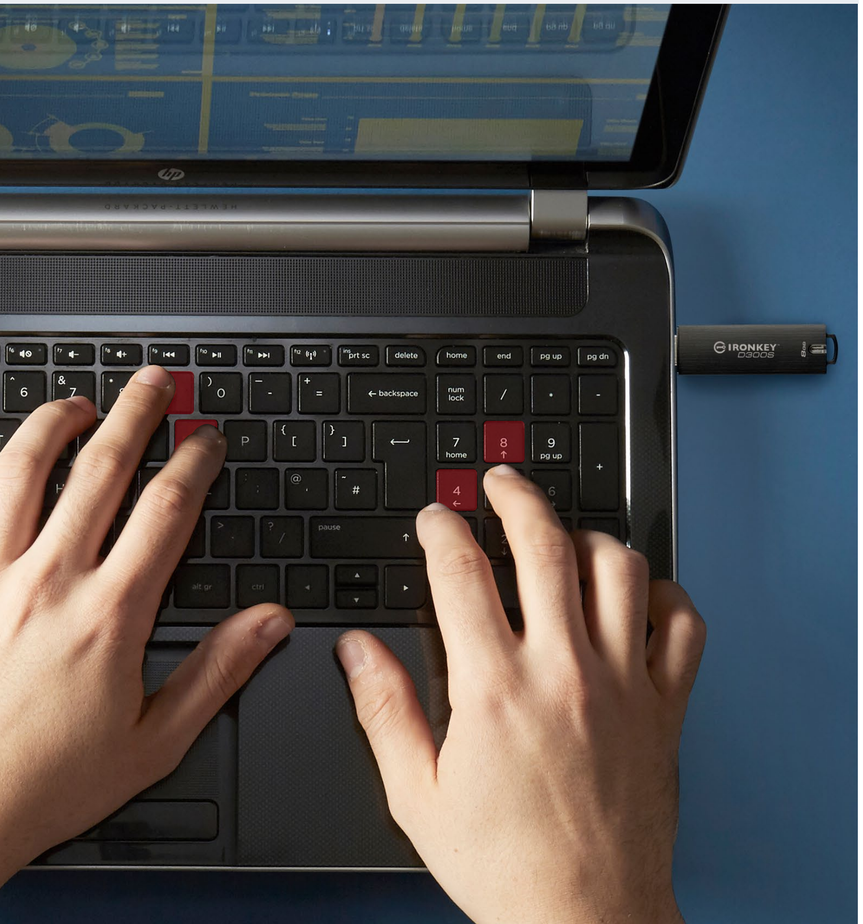
Sarah Janes
@SarahkJanes
Dyrektor zarządzająca Layer 8 Ltd

Źródło: Ankieta firmy Kingston, 2019 r.

Czy regularnie przeprowadzasz audyt pamięci zewnętrznych wykorzystywanych przez pracowników?

71%	11%	9%	9%
Tak	Nie	Nie mam pewności	Nie dotyczy

Część 4. Edukacja pracowników to konieczność



Edukacja to początek, a nie koniec

W wielu organizacjach brakuje wewnętrznych szkoleń w zakresie bezpieczeństwa, pojawiły się więc firmy wypełniające tę lukę. Należy jednak dokładnie sprawdzić tematykę szkolenia proponowanego przez zewnętrznych konsultantów. Często bowiem nie dotyczy ono cyberbezpieczeństwa, a zgodności z procedurami danej firmy (ponieważ na takie szkolenie firma uzyskała fundusze). Ryzykowne zachowania nie zostaną wyeliminowane, dopóki pracownicy nie zrozumieją istoty problemu.

Sarah Janes
@SarahkJanes

Dyrektor zarządzająca
Layer 8 Ltd

„Jeśli organizacja chce zmienić sposób działania pracowników, musi zapewnić profesjonalnie prowadzone szkolenia na temat podstaw bezpieczeństwa infrastruktury i cyberbezpieczeństwa".

Szkolenie nie może być wymówką. Myślenie, że skoro pracownicy zostali przeszkoleni, to automatycznie ich sposób postępowania będzie zgodny z procedurami bezpieczeństwa oraz przepisami jest sporym i niebezpiecznym uproszczeniem. Sukces wymaga nieustannej pracy nad właściwymi wzorcami zachowania i kulturą organizacji.

Rafael Bloom
@rafibloom73

Dyrektor firmy Salvatore Ltd

„Spotkałem się z przypadkami, gdzie w certyfikowanych firmach przechowywano pliki lub notatniki z hasłami bądź pracownicy zostawiali w samochodzie niezaszyfrowane kopie dysków twardych. Certyfikaty nie mają znaczenia, jeśli pracownicy nie rozumieją podstawowych zasad bezpieczeństwa".

Pracuj nad odpowiedzialnością na wszystkich poziomach

Jednym z elementów strategii wprowadzania koniecznych zmian w kulturze organizacyjnej jest wyznaczenie mentorów ds. cyberbezpieczeństwa. Ich zadaniem jest praca nad wyzwaniami związanymi z bezpieczeństwem i wprowadzanie zabezpieczeń na każdym poziomie struktury organizacyjnej firmy.

Sarah Janes
@SarahkJanes

Dyrektor zarządzająca
Layer 8 Ltd

„Rozmowy mentorów z pracownikami na temat wykonywanej przez nich pracy, połączone z dostępem do odpowiednich materiałów szkoleniowych, mogą ułatwić wprowadzanie zmian oraz promować model odpowiedzialnych zachowań".

Podsumowanie

Ochrona danych i cyberbezpieczeństwo mogą wydawać się uciążliwym obowiązkiem, jednak dzięki odpowiednim narzędziom, które można wdrożyć niskim kosztem, praca zdalna może być wykonywana przejrzyście i bezpiecznie. Należy jednak pamiętać, że w firmie muszą zostać wprowadzone zmiany w infrastrukturze oraz kulturze organizacyjnej, aby zespół zaczął stosować się do zasad bezpieczeństwa.

Podsumowując:

- Praca zdalna staje się coraz bardziej popularna i daje wiele korzyści, takich jak zwiększona produktywność, lojalność pracowników czy mniejsze koszty. Wiąże się z licznymi wyzwaniami związanymi z bezpieczeństwem.
- Naruszenie ochrony danych może prowadzić do poważnych konsekwencji, a nieprzestrzeganie RODO wiązać z wysokimi grzywnami ze strony UODO.
- Własne urządzenia (BYOD), niezabezpieczony sprzęt, nieprawidłowe korzystanie z oprogramowania oraz publicznych sieci Wi-Fi to powszechne zagrożenia dla bezpieczeństwa.
- Prawidłowo zbudowana infrastruktura powinna ułatwiać, a nie utrudniać skuteczność działań pracowników. W przeciwnym razie pracownicy będą starali się obejść zabezpieczenia.
- Zrób rozeznanie i wybierz sprawdzonych producentów oraz dostawców usług IT.
- Narzędzia, takie jak szyfrowane nośniki SSD czy pamięci USB, sieci VPN oraz programy do ochrony danych (DLP) są łatwe do wdrożenia i nie powinny stanowić dużego obciążenia finansowego dla firmy.
- Odpowiednia ochrona danych wymaga zmiany kultury organizacyjnej i promowanych zachowań w firmie. Pracownicy muszą rozumieć potrzebę działania zgodnie z ustalonymi zasadami, a nie tylko otrzymywać instrukcje, promujące nieświadome przestrzeganie protokołów.
- Zewnętrzni konsultanci mogą pomóc przeszkolić pracowników, jednak należy sprawdzić jakość materiałów szkoleniowych. Należy pamiętać, że pracownicy nie zaadoptują automatycznie koniecznych wzorców zachowań tylko dlatego, że dowiedzą się o tym podczas szkolenia.
- Należy powołać mentorów ds. cyberbezpieczeństwa, których zadaniem będzie omawianie wyzwań związanych z bezpieczeństwem oraz promowanie pożądanych wzorów zachowania na każdym szczeblu struktury organizacyjnej firmy.

O firmie Kingston

Przez 32 lat obecności na rynku firma Kingston zgromadziła wiedzę pozwalającą rozpoznawać i rozwiązywać wyzwania związane z pracą zdalną. Pozwala to jej pracownikom bezpiecznie wykonywać pracę z dowolnego miejsca, nie narażając przy tym przedsiębiorstwa na wysokie kary.

#KingstonIsWithYou