Przewodnik dotyczący przestrzegania przepisów rozporządzenia GDPR

Dostarczone przez

Spis treści

03 | Wprowadzenie

04 | Wyjaśnienie GDPR EU

07 | Wyzwania techniczne dotyczące przestrzegania przepisów

09 | Wdrażanie zabezpieczeń punktów końcowych

15 | Przygotowanie do GDPR

18 | Podsumowanie

Wprowadzenie

Nadszedł czas uwzględnienia ochrony prywatności w fazie projektowania rozwiązań.

25 maja 2018 roku wchodzi w życie Ogólne rozporządzenie UE o ochronie danych (General Data Protection Regulation, GDPR). Zastąpi ono wszystkie krajowe przepisy dotyczące ochrony danych w UE, a każdy, kto prowadzi działalność na wspólnym rynku, będzie musiał je zaakceptować. Obejmuje to firmy spoza UE, które chcą obsługiwać klientów w Unii Europejskiej.

GDPR wymaga, aby każde naruszenie danych osobowych było zgłaszane w ciągu 72 godzin. Nieprzestrzeganie tego wymagania lub zaniechanie może doprowadzić do nałożenia grzywny w wysokości do 20 mln EUR lub 4% globalnych obrotów firmy, w zależności od tego, która wartość jest większa.

Na szczęście środki wymagane do ochrony danych firmy jako całości służą również do zabezpieczania danych klientów. To samo podejście dotyczące ochrony punktów końcowych w wielu warstwach, które zaleca HP, pomoże zapewnić zgodność z GDPR.

W tym e-przewodniku zbadamy najważniejsze składniki GDPR, które muszą znać specjaliści IT i sprawdzimy, w jaki sposób program obsługi urządzeń końcowych zapewnia bezpieczeństwo.

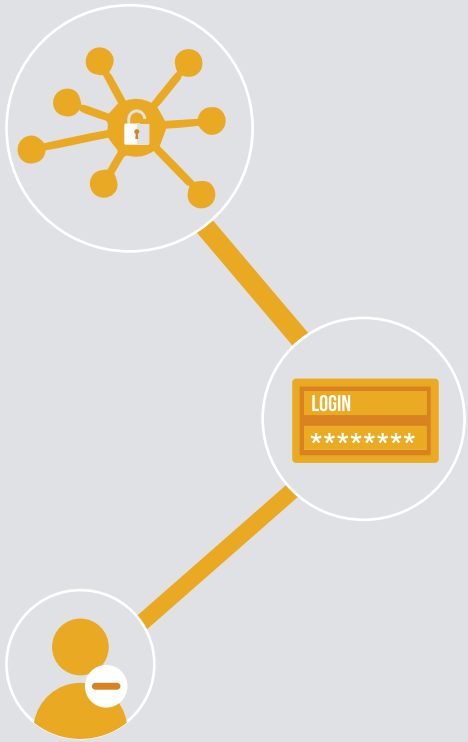
Wyjaśnienie GDPR EU

Kluczowe punkty dla działów IT

Istnieją zasadniczo dwa aspekty dotyczące GDPR: ochrona praw podmiotów i ochrona prywatności podmiotów w UE, których dane dotyczą. Oba te zagadnienia mają swoje technologiczne implikacje.

Aby poznać szczegóły, należy przeczytać cały tekst. Jednak w przypadku decydentów w dziedzinie IT są to punkty, które trzeba znać:

1. **Naruszenia bezpieczeństwa muszą być zgłoszone w ciągu 72 godzin**
   Jeśli nastąpi naruszenie bezpieczeństwa danych, powinno to nastąpić w ciągu 72 godzin od jego wykrycia. Kary za zaniechanie zgłoszenia są wysokie (zobacz punkt 5 „Jakie są kary za nieprzestrzeganie przepisów?")
2. **Prawo do bycia zapomnianym (usunięcie danych)**
   Każdy podmiot UE, którego dotyczą dane, ma prawo zostać zapomnianym. Na żądanie należy usunąć jego dane wraz ze wszystkimi kopiami.
3. **Prawo do przenoszenia danych**
   Rezydenci UE mają prawo do kontroli swoich danych. Na żądanie należy dostarczyć im dane w dostępnym formacie, w którym będą mogli je przesłać stronie trzeciej
4. **Transfery międzynarodowe**
   Przeniesienie danych personelu do innej jurysdykcji danych (np. poza UE) może być wykonane tylko za wyraźną zgodą i tylko do organów regulacyjnych uznanych za „odpowiednie" lub z zapewnieniem dodatkowych zabezpieczeń[1]
5. **Uwzględnienie ochrony prywatności w fazie projektowania**
   Organizacje muszą przyjąć podejście polegające na uwzględnieniu ochrony prywatności w fazie projektu, które domyślnie integruje bezpieczeństwo danych w produktach, procesach i usługach[2,3]



Kogo dotyczy GDPR?

Rozporządzenie GDPR dotyczy każdej firmy, która gromadzi i/lub przetwarza dane osobowe rezydentów UE. Obejmuje to organizacje znajdujące się poza UE, które działają w UE.

[1]https://iapp.org/news/a/top-10-operational impacts-of-the-gdpr-part-4-cross-border-data-transfers/ [2]Allen & Overy — The EU General Data Protection Regulation 2016
[3]http://www.computerweekly.com/news/450296306/10-key-facts-businesses-need-to-note-about-the-GDPR

Wyjaśnienie GDPR EU

Co jest uznawane za dane osobowe?

W rozumieniu GDPR dane osobowe obejmują „dowolne dane, które mogą być wykorzystane do zidentyfikowania osoby".

Poza informacjami tradycyjnie uważanymi za identyfikujące obejmuje to informacje genetyczne, psychiczne, kulturowe, gospodarcze lub społeczne.

Może to sprawić, że GDPR będą podlegać organizacje wyłączone wcześniej z prawodawstwa dotyczącego ochrony danych.

Jakie są kary za nieprzestrzeganie przepisów?

Maksymalna grzywna wynosi 20 mln EUR lub 4% globalnych obrotów firmy, w zależności od tego, która wartość jest większa. Dotyczy to najpoważniejszych przestępstw objętych rozporządzeniem, takich jak brak zgłoszenia naruszenia bezpieczeństwa w ciągu 72 godzin od jego wykrycia.

Za mniej poważne wykroczenia grzywna wynosi maksymalnie 10 mln EUR lub 2% globalnych obrotów firmy. Nie trzeba dodawać, że koszty nieprzestrzegania przepisów są znaczne.

Lista kontrolna procedur GDPR

W ramach zarządzania danymi będą potrzebne wyraźne procedury dotyczące:

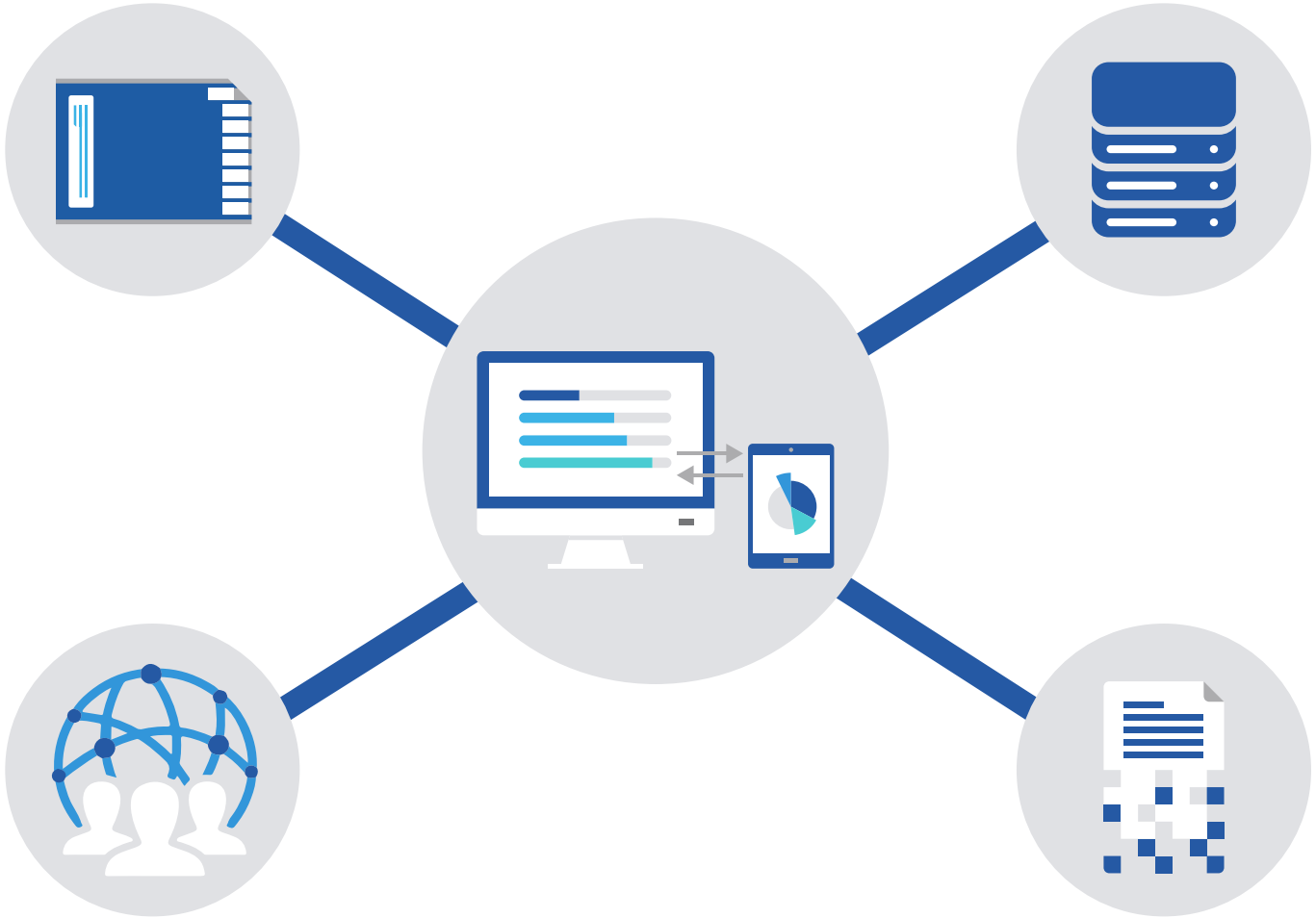
- Informowania podmiotów, których dotyczą dane, o tym, jak ich dane będą gromadzone, przechowywane i przetwarzane
- Uzyskiwania wyraźnej zgody podmiotów, których dotyczą dane
- Udostępniania danych podmiotów w dostępnym dla nich formacie
- Usuwania wszystkich danych osobowych podmiotu, którego dane dotyczą, w tym kopii
- Przenoszenia danych do innego operatora lub organizacji je przetwarzającej
- Przenoszenia danych poza UE — również w obrębie organizacji

Wyzwania techniczne dotyczące przestrzegania przepisów

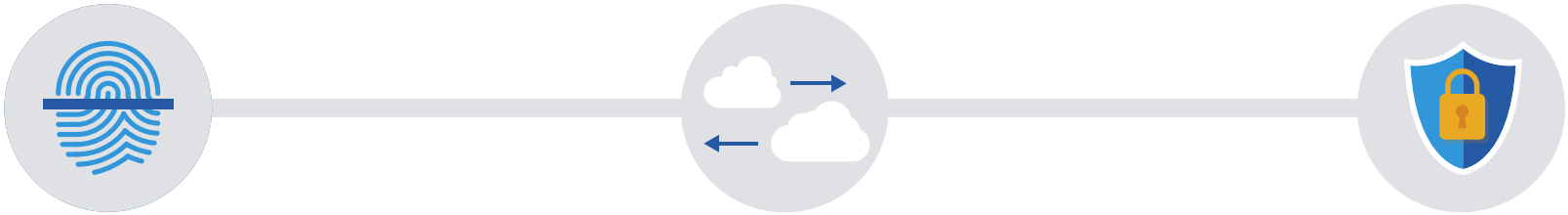
Największe wyzwania GDPR mają charakter techniczny.

Umożliwienie przenoszenia danych, ochrony danych osobowych i prawa do ich zapomnienia wymaga obszernej mapy lokalizacji i dostępu aż do poziomu urządzenia.

Ponieważ zagrożenie cyberprzestępczością rośnie z roku na rok, utrzymanie absolutnego bezpieczeństwa jest coraz większym wyzwaniem.



Wyzwania techniczne dotyczące przestrzegania przepisów



Śledzenie urządzeń

Przestrzeganie prawa do przenoszenia danych i do ich zapominania wymaga szczegółowego opisu wszystkich danych osobowych przechowywanych przez organizację.

Należy znać:

- Każde urządzenie, na którym są przechowywane dane osobowe
- Każde urządzenie, które ma dostęp do danych osobowych

Jest to jedyny sposób zagwarantowania, że można pobrać i/lub usunąć dane osobowe przechowywane przez firmę.

Śledzenie chmur

Przeciętne europejskie przedsiębiorstwo wykorzystuje 608 aplikacji, liczba ta jest w 90% niedoszacowana. Pracownicy często bez wiedzy działu IT używają komercyjnych aplikacji dostępnych w chmurze.[4]

Zgodność z GDPR wymaga, aby używanie chmury było ograniczone do usług, które:

- Znajdują się w obrębie UE i dlatego zachowują zgodność z GDPR
- Znajdują się pod jurysdykcją organu regulującego ochronę danych uznawaną za „odpowiednią" przez UE

Wszystkie inne lokalizacje mogą naruszać zasadę transferu międzynarodowego. Należy wiedzieć, jakich usług w chmurze używają pracownicy, aby powołać się na prawo do zapomnienia.

Ochrona danych

Rośnie zagrożenie cyberprzestępczością. Nie tylko dlatego, że rośnie też wykorzystanie niezabezpieczonych urządzeń sieciowych i osobistych.

Naruszenia są niemal nieuniknione. W UE jest to wiadome. Ale aby uniknąć kosztownych kar, należy:

- Wdrożyć narzędzie do monitorowania zdarzeń (Systems Incident Event Monitoring, SIEM), aby zgłosić naruszenie w ciągu 72 godzin
- Wdrożyć wielowarstwową ochronę punktów końcowych, aby wykazać należytą staranność w zapobieganiu naruszeniom

Użytkownicy również muszą być świadomi swoich obowiązków i nie używać niezatwierdzonych urządzeń i sieci.

[4]https://www.cloudindustryforum.org/content/cloud-and-eu-gdpr-six-steps-compliance

Zagrożenie cyberprzestępczością

Cyberprzestępczość jest realnym, obecnym i rosnącym zagrożeniem

82%

organizacji doświadczyło zagrożenia/naruszenia w ciągu 12 miesięcy[5]

80%

specjalistów IT przewiduje wzrost zagrożeń w ciągu najbliższych trzech lat[6]

78%

firm zgłasza wzrost liczby ataków w ciągu ostatnich pięciu lat[7]

60%

liderów IT zauważa, że cyberprzestępczość pokonuje ich linie obrony[8]

81%

firm ocenia wewnętrzne zaniedbania jako największe zagrożenie dla cyberbezpieczeństwa[9]

81%

liderów IT twierdzi, że urządzenia przenośne w ich sieciach były celem oprogramowania typu malware[9]

72%

twierdzi, że pozwolenie pracownikowi na używanie komercyjnego oprogramowania w chmurze jest ryzykowne[9]

69%

twierdzi, że wprowadzenie BYOD stanowi ryzyko dla bezpieczeństwa

[5]HPI Printer Security Research 2016 (Spiceworks) [6]HP Printer Security Report 2015 [7] Ponemon 2016 State of the Endpoint Report [8]IBM CISO Assessment 2014 [9]Ponemon 2016 State of the Endpoint Report

Wdrażanie zabezpieczeń urządzeń końcowych

Wielowarstwowe podejście HP do zabezpieczania punktów końcowych

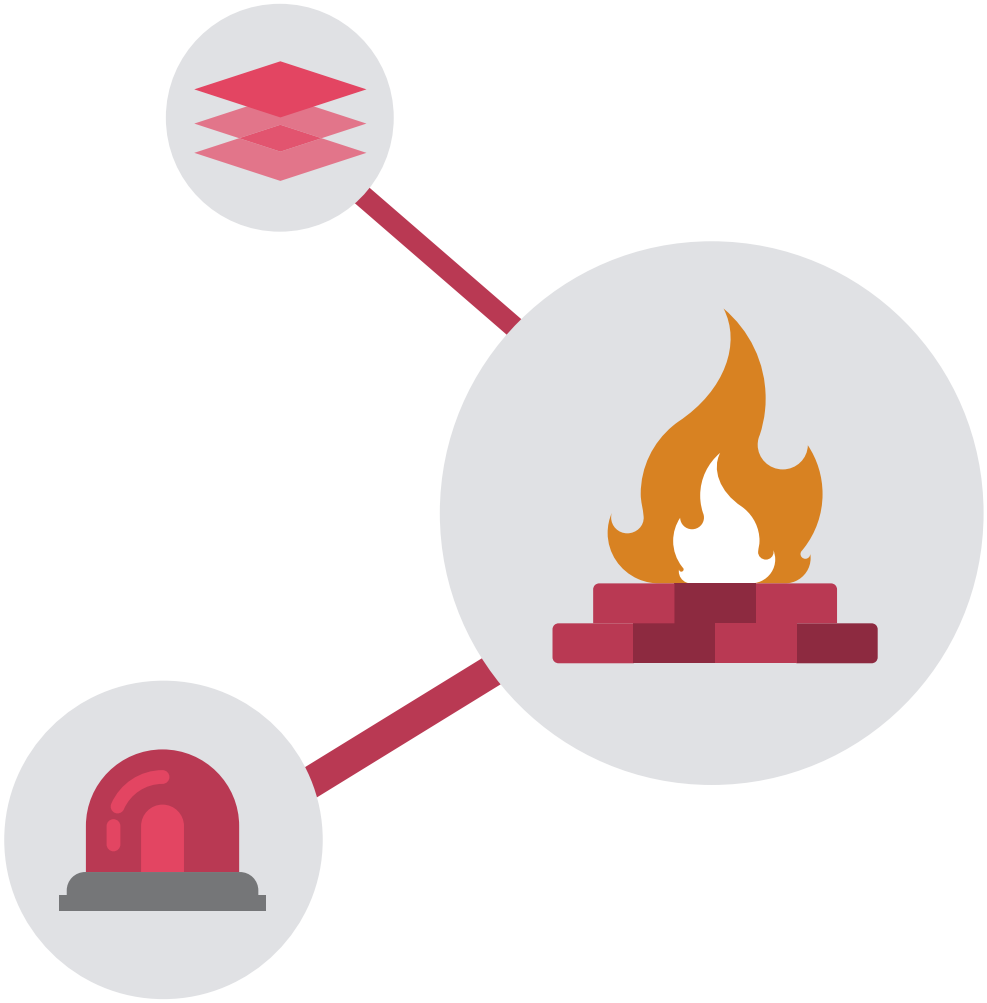
Podejście do cyberbezpieczeństwa polegające na zapobieganiu i ochronie — zapora i program antywirusowy już nie wystarczają. I nigdy nie wystarczały. W badaniach prowadzonych przez firmę Damballa wykazano, że oprogramowanie antywirusowe potrzebowało 6 miesięcy na zidentyfikowanie i usunięcie 100% złośliwych plików.[10]

W HP uważamy, że cyberbezpieczeństwo musi być wielowarstwowe, obejmować sieć, urządzenie i użytkownika oraz zapewniać wiele linii obrony w każdym z tych zakresów. Wykrywanie i reagowanie powinny mieć pierwszeństwo nad ochroną i obroną. Punkty końcowe są tymi, od których należy zacząć: zarówno urządzenie, jak i użytkownik.

Critical Security Controls (CSC)

W Centrum Bezpieczeństwa Internetowego (Center for Internet Security, CIS) zdefiniowano 20 uznanych w skali międzynarodowej krytycznych zabezpieczeń (Critical Security Controls, CSC) opracowanych, dopracowanych i zatwierdzonych przez czołowych ekspertów ds. bezpieczeństwa IT na całym świecie. Są one postrzegane jako ważne elementy higieny cyberprzestrzeni dla każdej organizacji.

Odwołaliśmy się do kluczowych zabezpieczeń CSC pod kątem zgodności z GDPR, ponieważ są to użyteczne wytyczne, ale pełny tekst jest dostępny online. Można go pobrać bezpłatnie z naszej biblioteki CIS.



[10]https://www.damballa.com/time-to-fix-malware-strategies-2/

Bezpieczeństwo sieciowe

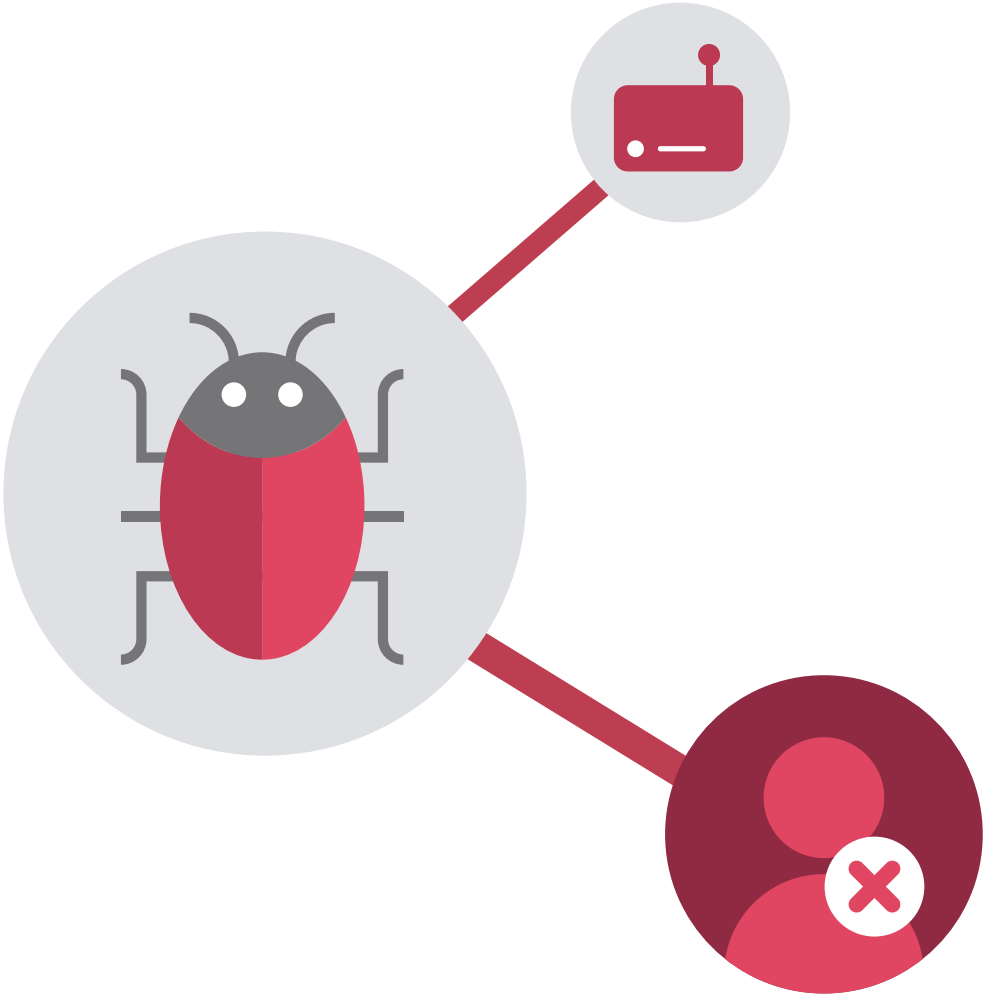
Większość hakerów zazwyczaj wykorzystuje pojedynczy punkt wejścia, aby uzyskać dostęp do całej sieci. Aby temu zapobiec, należy zatem zapewnić bezpieczeństwo na poziomie sieci.

- **Kontrola uprawnień administracyjnych (CSC 5)**
  Ograniczenie możliwości zmiany ustawień sieciowych i haseł do kilku osób
- **Kontrola dostępu w oparciu o zasadę ścisłej potrzeby (CSC 14)**
  Dostęp do poufnych informacji na temat użytkownika, urządzenia i lokalizacji. Ocena zagrożenia w stosunku do wrażliwości danych
- **Ograniczenie i kontrola portów sieciowych, protokołów i usług (CSC 9)**
  Wyłączenie wszystkich niepotrzebnych punktów dostępu, wirtualnych i fizycznych, w tym FTP, Telnet i usług drukowania
- **Utrzymywanie, monitorowanie i analiza rejestrów audytu (CSC 6)**
  Regularne przeglądanie rejestrów audytu w celu analizy zachowania systemu i wykrycia podejrzanych działań
- **Ciągłe testowanie podatności i jej minimalizowanie (CSC 4)**
  Ciągła ocena środowiska w zakresie jego podatności i podejmowanie działań mających na celu poprawę wyników, minimalizację możliwości naruszeń

Celem jest podział sieci pod kątem wrażliwości informacji. Żądania dostępu są oceniane pod kątem zagrożeń dla bezpieczeństwa. Nierozpoznane urządzenia, użytkownicy i żądania z niezabezpieczonych sieci są blokowane przy próbie dostępu do najbardziej wrażliwych informacji. Polityka BeyondCorp firmy Google jest dobrym modelem.[11]

[11]https://research.google.com/pubs/pub43231.html

Bezpieczeństwo sieciowe



Każde urządzenie jest potencjalną luką, zarówno firmowe, jak i osobiste. Trzeba znać każdy telefon, tablet, laptop i komputer stacjonarny, który ma dostęp do danych firmy.

- **Inwentaryzacja autoryzowanych i nieautoryzowanych urządzeń (CSC 1)**
  Przeprowadzenie audytu każdego urządzenia, które ma dostęp do danych
- **Inwentaryzacja autoryzowanego i nieautoryzowanego oprogramowania (CSC 2)**
  Przeprowadzenie audytu każdej aplikacji używanej w sieci — do bezpośredniego lub pośredniego dostępu do danych
- **Ochrona przed złośliwym kodem (CSC 8)**
  Zapewnienie, że każde urządzenie ma aktualną wersję programu antywirusowego i zabezpieczającego przed złośliwym kodem. Zapewnienie regularnego skanowania i aktualizacji

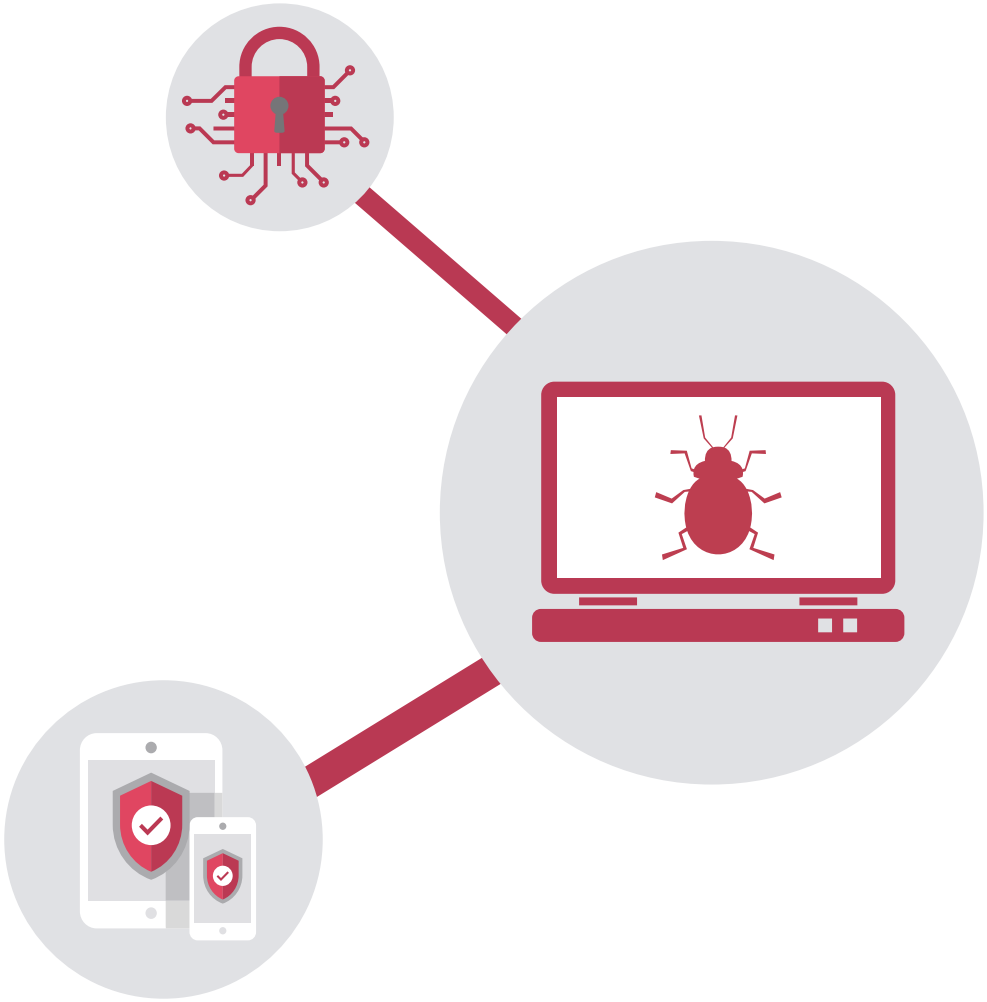
Zabezpieczanie urządzeń

Ponadto w działach IT należy rozważyć dodatkowe kontrole:

- **Wieloskładnikowe uwierzytelnianie**
  Zapewnienie, że każde urządzenie robocze jest zabezpieczone. Najlepiej oprócz haseł jest używać uwierzytelniania biometrycznego (patrz 14 „Urządzenia z ochroną prywatności uwzględnioną w fazie projektowania”)
- **Zdalny dostęp**
  Zapewnienie zdalnego dostępu do urządzenia umożliwiającego pobieranie lub usuwanie danych osobowych, zastosowanie kwarantanny i zakończenie procesów, a także wyłączenie i zablokowanie urządzenia w przypadku jego utraty lub kradzieży (patrz 14 „Wykrywanie i reakcja”)
- **Zapoznanie każdego pracownika z protokołami i procedurami bezpieczeństwa**
  Upewnienie się, że każdy pracownik jest świadomy zagrożeń i zna swoje obowiązki związane z cyberbezpieczeństwem, w tym zgłaszanie podejrzanych działań
- **Prowadzenie aktywnych szkoleń w zakresie bezpieczeństwa w sieci**
  Organizowanie warsztatów, seminariów, prowadzenie ćwiczeń dotyczących wyłudzania danych, tak aby każdy wiedział, jak uniknąć podstawowych błędów i jak zachować zgodność z GDPR
- **Minimalizowanie użycia osobistych urządzeń/aplikacji**
  Należy zniechęcać do używania osobistych urządzeń i aplikacji w pracy. Skorzystanie z pomocy wszechstronnych i elastycznych zasad CYOD

Wdrożenie takiego systemu zabezpieczeń powinno pomóc w utrzymaniu kontroli nad urządzeniami firmowymi, aby chronić dane i ułatwiać egzekwowanie prawa do przenoszenia danych oraz do ich zapominania.

Aby dowiedzieć się więcej o wielowarstwowym podejściu HP do bezpieczeństwa, można przeczytać nasze opracowanie Security Begins at the Endpoint.



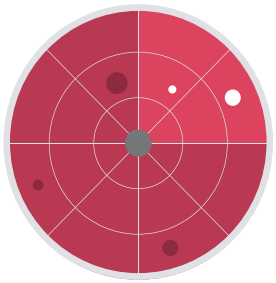
Dlaczego każdy pracownik powinien być świadomy zagrożeń cybernetycznych

58% zagrożeń cybernetycznych jest umożliwianych przez pracowników, byłych pracowników i zaufanych partnerów.[12] Zabezpieczenie każdego urządzenia oznacza także zabezpieczenie jego użytkownika.

- Krajowy Komitet Partii Demokratycznej w USA (U.S. Democratic National Committee, DNC) padł ofiarą ataku hakerskiego w 2016 roku, gdy John Podesta kliknął link phishingowy błędnie oznaczony przez asystenta jako prawidłowy[13]
- Zdjęcia nagich celebrytów zalały Internet w 2014 roku, po tym jak 36-letni Ryan Collins uzyskał dostęp do iCloud Jennifer Lawrence i innych za pomocą prostych phishingowych wiadomości e-mail wysłanych z urządzenia Apple.[14]
- W 2012 roku wyciekło 68 mln haseł do usługi Dropbox, ponieważ pewien pracownik użył tego samego hasła do wewnętrznych systemów oraz do swojego konta LinkedIn[15]
- Prezydent Donald Trump nadal używa standardowego telefonu Samsung Galaxy. Eksperci nie zastanawiają się, czy padł już ofiarą hakerów, ale raczej jak wiele obcych agencji wywiadowczych już to zrobiło[16]

[12]http://www.clearswift.com/sites/default/files/images/blog/enemy-within.pdf [13]https://www.theguardian.com/us-news/2016/dec/14/dnc-hillary-clinton-emails-hacked-russia-aide-typo-investigation-finds [14]http://www.forbes.com/sites/thomasbrewster/2016/03/16/icloud-hacking-jennifer-lawrence-fappening-apple-nude-photo-leaks/#45fed5d77b88 [15]https://www.theguardian.com/technology/2016/aug/31/dropbox-hack-passwords-68m-data-breach [16]https://www.theguardian.com/commentisfree/2017/feb/19/if-trump-hates-leaks-needs-to-give-up-phone

Wykrywanie i reagowanie

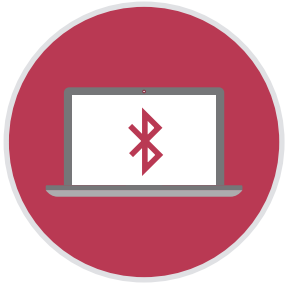


Wykrywanie i reagowanie to ramy cyberbezpieczeństwa, w których całkowite zapobieganie jest prawie niemożliwe.

Ważna jest wiedza (wykrycie), że nastąpiło naruszenie oraz podjęcie natychmiastowych działań (reakcja).

Dostępne jest oprogramowanie, które zmienia każde urządzenie w czujnik czasu rzeczywistego, co pozwala administratorowi reagować, np. wyłączając urządzenia, poddając kwarantannie pliki i usuwając dane.

Urządzenia z ochroną prywatności uwzględnioną w fazie projektowania



Urządzenia HP z ochroną prywatności wbudowaną w fazie projektowania.

Funkcje zabezpieczeń obejmują pierwszy na świecie system samonaprawy, automatyczną funkcję blokady Bluetooth, która blokuje urządzenie, gdy użytkownik wychodzi, oraz zintegrowane ekrany zapewniające prywatność.

Te funkcje same z siebie nie zapewniają zgodności z GDPR, ale na pewno w tym pomagają.

Przygotowanie do GDPR

Praktyczne kroki, które można podjąć już teraz

Rozporządzenie GDPR wchodzi w życie 25 maja 2018 r. Nadszedł czas na przygotowanie, ale jak już wiadomo, jest wiele do zrobienia.

Pierwszy krok to **audyt bieżącej sytuacji, jeśli chodzi o dane**. Należy ocenić miejsca, w których są przechowywane dane, z których są kopiowane i kto ma do nich dostęp. Jeśli są wykorzystywane rozwiązania w chmurze, należy dowiedzieć się, gdzie znajdują się serwery i czy są zgodne z GDPR. To samo dotyczy każdej usługi SaaS lub innych organizacji partnerskich, z którymi nawiązuje się współpracę i udostępnia dane. To pokazuje, ile potrzeba zmian w celu zapewnienia zgodności

Opracowanie zasad dotyczących danych Opracowanie szczegółowych procedur i protokołów dotyczących przechowywania danych, określenie, kto ma do nich dostęp i może je kopiować poza firmą lub za granicą w obrębie firm międzynarodowych

Opracowanie procedur pobierania i usuwania danych osobowych Przekazanie ich do wiadomości wszystkich osób w firmie Prowadzenie sesji szkoleniowych Podkreślanie ich ważności

Opracowanie zasad bezpieczeństwa Utworzenie nowych ram cyberbezpieczeństwa działających na zasadzie wykrywania i reagowania w punktach końcowych Jeśli to konieczne, przeanalizowanie zasad bezpieczeństwa urządzeń Jeśli to konieczne, inwestowanie w nowe technologie Tylko 36% specjalistów IT uważa, że ma wystarczająco duży budżet na zapewnienie bezpieczeństwa punktów końcowych.[17] Kary z tytułu GDPR mogą wreszcie zachęcić osoby zarządzające firmami, aby to zmienić.

[17]Ponemon 2016 State of the Endpoint Report

Przygotowanie do GDPR

Lista kontrolna GDPR

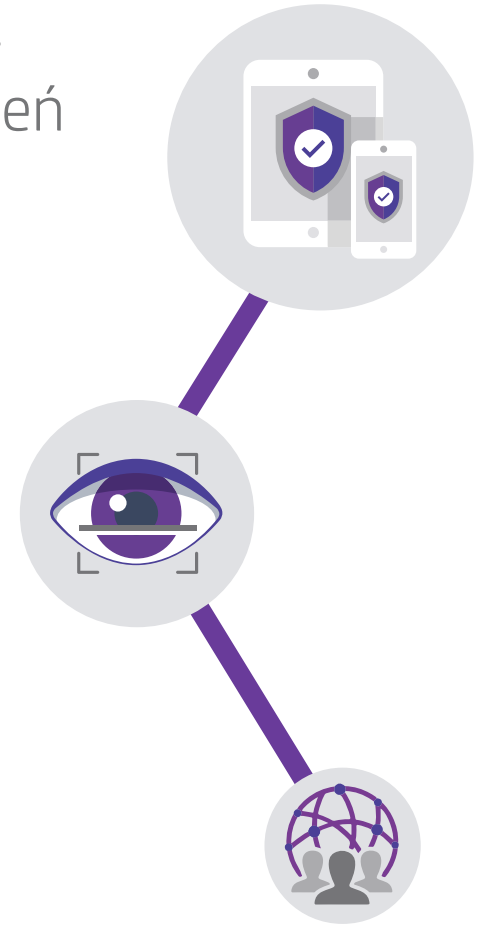
5 kluczowych kroków w kierunku zgodności z GDPR

1. Jeśli to konieczne, powołanie osoby, która będzie odpowiedzialna za dane, np. inspektora ochrony danych (Data Protection Officer, DPO)
2. Wykonanie pełnego audytu danych, w tym zbadanie referencji dostawców usług Cloud i SaaS w odniesieniu do GDPR
3. Utworzenie nowych ram zarządzania danymi, w tym procedur przenoszenia danych i prawa do zapomnienia
4. Utworzenie nowych ram cyberbezpieczeństwa, wdrożenie wielowarstwowych zabezpieczeń punktów końcowych
5. Przekazanie zasad i protokołów do wiadomości wszystkich osób w firmie

Lista kontrolna bezpieczeństwa urządzeń

6 kluczowych kroków do zabezpieczenia punktów końcowych

1. Wykonanie audytu wszystkich autoryzowanych i nieautoryzowanych urządzeń z dostępem do danych osobowych
2. Inwestowanie w nowe bezpieczniejsze urządzenia, jeśli to konieczne
3. Wdrożenie zdalnego dostępu i usuwanie uprawnień do danych firmowych na urządzeniach
4. Wdrożenie polityki regularnego skanowania i aktualizacji oprogramowania zabezpieczającego
5. Wdrożenie oprogramowania do wykrywania i reagowania w czasie rzeczywistym
6. Szkolenie pracowników w zakresie cyberbezpieczeństwa



Kalendarz bezpieczeństwa urządzeń końcowych

Podstawowy harmonogram wdrażania zabezpieczeń punktów końcowych według GDPR

2017

Maj

Wyznaczenie menedżera projektu, który będzie odpowiadał za zabezpieczenie punktów końcowych

Czerwiec

Przeprowadzenie audytu bieżących zasad bezpieczeństwa, praktyk i urządzeń

Lipiec

Ustalenie wymagań sprzętowych i zasad bezpieczeństwa dla punktów końcowych (CYOD/BYOD itp.)

Sierpień

Wybór oprogramowania do wykrywania problemów z zabezpieczeniami i reagowania na nie

Wrzesień

Zaprojektowanie wielowarstwowego systemu dostępu do danych firmy

Październik

Zaprojektowanie chmury publicznej/prywatnej, aby umożliwić odpowiedni dostęp do danych podczas przebywania poza biurem

Listopad

Zaprojektowanie programu szkolenia dla użytkowników obejmującego regularne sprawdzanie obecności oprogramowania wyłudzającego informacje

Grudzień

Ogłoszenie nowych zasad bezpieczeństwa w całym przedsiębiorstwie

2018

Styczeń

Zaimplementowanie nowej architektury danych w chmurze publicznej/prywatnej

Luty

Zaimplementowanie nowych zasad bezpieczeństwa urządzeń

Marzec

Zaimplementowanie wykrywania oprogramowania i reagowania na nie

Kwiecień

Przeprowadzenie szkolenia dla użytkowników obejmującego zasady powiązane z GDPR

Maj

GDPR wchodzi w życie

Podsumowanie

GDPR nadchodzi

Jeśli macie szczęście, w Waszej organizacji spełnionych jest już wiele regulacji z nowych przepisów — jest to, w dużej mierze, jedynie ujęcie w ramy tego, co stanowi najlepsze praktyki.

Natomiast jeśli Wasza organizacja działała w wielu krajach UE, mogliście spotkać się z bardziej surowymi środkami.

Środki bezpieczeństwa, które zalecamy, aby dostosować się do GDPR, pomogą zapobiec naruszeniom, które mogłyby być niezwykle kosztowne dla organizacji. Według ostatnich obliczeń brytyjski rząd szacuje, że brytyjskie przedsiębiorstwa straciły 21 mld funtów w ciągu jednego roku. Oczekuje się, że ta liczba jeszcze wzrośnie.[18]

Ponadto wiele środków wymaganych do zapewnienia naprawdę stabilnego bezpieczeństwa przyczyni się również do spełnienia innych aspektów GDPR. Ograniczenie dostępu do danych poszczególnym użytkownikom, urządzeniom i sieciom nie tylko minimalizuje ryzyko utraty danych, ale także ułatwia śledzenie danych osobowych. Zapewnia to także prawo do przenoszenia danych i do ich zapomnienia, nie wspominając już o transferach międzynarodowych.

Ten e-przewodnik to dopiero początek. Bezpieczeństwo zawsze było priorytetem dla HP. Ochrona prywatności uwzględniona w fazie projektowania to nasza polityka na lata. Teraz, gdy jest to wymagane, a nie pożądane, jesteśmy dobrze przygotowani, aby pomóc przyjąć takie samo podejście.

Aby dowiedzieć się więcej na temat HP i naszych produktów, które mogą pomóc zapewnić zgodność z GDPR, można odwiedzić **naszą stronę Privacy by Design**

[18]https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the cost-of-cyber-crime-full-report.pdf