DOBRE PRAKTYKI

DLA KADRY ZARZĄDZAJĄCEJ

DOBRE PRAKTYKI DLA KADRY ZARZĄDZAJĄCEJ SĄ ELEMENTEM STANDARDU CYBERBEZPIECZEŃSTWA PPBW DLA MAŁYCH I ŚREDNICH PRZEDSIĘBIORSTW ORAZ INSTYTUCJI PUBLICZNYCH, OPRACOWANEGO PRZEZ POLSKĄ PLATFORMĘ BEZPIECZEŃSTWA WEWNĘTRZNEGO.

SPIS TREŚCI

03

ZABEZPIECZENIE STACJI ROBOCZYCH I UŻYTKOWNIKÓW

Opracuj politykę dotyczącą informowania pracowników o zagrożeniach

Przygotuj politykę, która będzie regulować kiedy i w jaki sposób pracownicy powinni być informowani o zagrożeniach, trwających atakach i zalecanym sposobie reakcji. Polityka powinna regulować:

- w jakich sytuacjach użytkownicy powinni być powiadamiani (np. trwający atak phishingowy, wykrycie luki w używanym oprogramowaniu, itp),
- kto powinien przesyłać informacje (zazwyczaj dział IT),
- w jaki sposób informacje powinny być przesyłane (np. lista mailingowa).

WYJAŚNIENIE

Dzięki dobrej komunikacji dotyczących aktualnych zagrożeń pracownicy będą mogli lepiej na nie zareagować, wzrośnie też ich świadomość zagrożeń i czujność.

Dbaj o regularne szkolenia i poszerzanie świadomości zagrożeń pracowników

Dbaj o regularne szkolenia i przygotowanie pracowników do radzenia sobie z możliwymi zagrożeniami. Można to realizować na wiele sposobów, poza standardowymi szkoleniami można korzystać z kursów internetowych, wprowadzić regularne przesyłanie na listę mailingową krótkich porad dotyczących bezpieczeństwa, itp.

WYJAŚNIENIE

Zazwyczaj najsłabszym ogniwem systemów jest człowiek i bardzo wiele ataków opiera się na socjotechnice. Z tego względu należy dbać o odpowiednie przygotowanie pracowników.

04

ZABEZPIECZENIE STACJI ROBOCZYCH I UŻYTKOWNIKÓW

Opracuj politykę dotyczącą podłączania urządzeń przenośnych

W zależności od ważności danych oraz potrzeb firmy można:

- całkowicie zakazać używania przenośnych nośników danych,
- pozwolić na korzystanie tylko z firmowego, szyfrowanego i zabezpieczonego sprzętu,
- wprowadzić wymagania dotyczące używanych nośników danych (szyfrowanie, zakaz wynoszenia poza firmę, zakaz podłączania do niezaufanych komputerów),
- wprowadzić ograniczenie dotyczące tego jakie dane mogą być kopiowane na przenośne nośniki.

Za opracowaną polityką powinny również iść rozwiązania techniczne wdrażane przez administratorów. W zależności od wybranej polityki może to być na przykład:

- całkowita blokada portów USB,
- zainstalowanie oprogramowania monitorującego podpinane urządzenia,
- obowiązkowe skanowanie urządzeń antywirusem po podłączeniu,
- inwentaryzacja urządzeń oraz danych, które są na nich przechowywane, aby w razie zgubienia lub kradzieży któregoś urządzenia móc oszacować potencjalne ryzyko.

WYJAŚNIENIE

Urządzenia przenośne, takie jak pendrive, karty SD, dyski przenośne, telefony niosą ze sobą wiele zagrożeń, m.in.:

- zainfekowanie komputera złośliwym oprogramowaniem – przypadkowe lub celowe przez atakujących firmę,
- wyciek danych z firmy,
- utratę kontroli nad przechowywaniem i kontrolą dostępu do danych w związku z dużą liczbą przenośnych nośników.

W związku z tym należy opracować politykę regulującą podłączanie takich przenośnych nośników danych.

05

ZABEZPIECZENIE STACJI ROBOCZYCH I UŻYTKOWNIKÓW

Opracuj procedurę reagowania na nieznane i niezaufane nośniki danych/urządzenia

Opracuj procedurę, która będzie regulowała reakcję na nieznane i niezaufane nośniki danych lub urządzenia. Zazwyczaj odpowiednim postępowaniem jest przekazanie nośnika administratorom, aby zbadali go w bezpiecznych warunkach.

WYJAŚNIENIE

Pojawienie się nieznanych i niezaufanych nośników danych/urządzeń może oznaczać próbę ataku bazująca na podrzuceniu takiego sprzętu do firmy w nadziei na to, że zostanie on podłączony do komputera. Opracowana procedura ułatwi pracownikom reagowanie na takie sytuacje.

Opracuj procedurę reagowania na wykryte przez antywirus zagrożenia

Poprawną reakcją jest natychmiastowe zgłoszenie incydentu działowi IT, który następnie może dokonać głębszej analizy i odpowiednio zareagować.

WYJAŚNIENIE

Dzięki opracowanej procedurze użytkownik będzie wiedział jak zareagować na zgłoszone przez antywirus zagrożenie i w efekcie dział IT będzie mógł szybciej zareagować.

06

ZABEZPIECZENIE STACJI ROBOCZYCH I UŻYTKOWNIKÓW

Opracuj politykę dotycząca instalacji oprogramowania przez użytkowników stacji roboczych

Przygotuj politykę regulującą instalowanie oprogramowania przez użytkowników stacji roboczych. Najbezpieczniejszym podejściem jest zezwolenie na instalowanie oprogramowania tylko z tzw. białej listy (whitelist), czyli listy zaufanych programów. W takim podejściu jeśli użytkownik chce zainstalować nowy program to musi najpierw poprosić dział IT o jego zweryfikowanie i dodanie do listy. Alternatywnym podejściem jest blokowanie instalacji oprogramowania z tzw. czarnej listy (blacklist), czyli listy złośliwych programów. Jest to rozwiązanie pozwalające na większą elastyczność, ale jednocześnie niosące za sobą większe ryzyko.

WYJAŚNIENIE

Jednym ze źródeł zagrożeń jest nieświadome zainstalowanie przez pracownika programu zainfekowanego lub podatnego na ataki.

Wdróż regularne kontrole aktualności oprogramowania oraz antywirusa

W porozumieniu z administratorami przygotuj odpowiednią dla firmy procedurę regularnej kontroli aktualności oprogramowania.

WYJAŚNIENIE

Dbanie o aktualizacje – zwłaszcza systemów podłączonych do sieci Internet – to pewne minimum dbania o bezpieczeństwo infrastruktury. Zapewnia nam to najczęściej ochronę przed większością powszechnie znanych (a więc często najłatwiejszych do wykorzystania) podatności i błędów.

07

BEZPIECZEŃSTWO PRACY ZDALNEJ I URZĄDZEŃ MOBILNYCH

Zadbaj o dostarczenie pracownikom możliwości korzystania z VPN

Jeśli pracownicy pracujący zdalnie mają dostęp do wrażliwych danych i usług warto zapewnić im możliwość korzystania z wirtualnej sieci prywatnej (VPN) oraz wprowadzić politykę obowiązkowego korzystania z niej.

WYJAŚNIENIE

VPN znacząco zwiększa bezpieczeństwo przesyłu danych (patrz Poradnik techniczny: VPN).

Określ wymagania bezpieczeństwa wobec urządzeń używanych do pracy zdalnej

Stwórz politykę regulującą wymagania bezpieczeństwa wobec urządzeń używanych do pracy zdalnej. Urządzenia te powinny posiadać poziom zabezpieczeń odpowiedni do dostępów jakie można z nich uzyskać. Jednym z podstawowych zabezpieczeń jest szyfrowanie dysku.

WYJAŚNIENIE

Korzystanie do pracy zdalnej z urządzeń niespełniających wymagań bezpieczeństwa może znacząco zwiększyć ryzyko wycieku danych lub włamania do usług firmowych.

08

BEZPIECZEŃSTWO PRACY ZDALNEJ I URZĄDZEŃ MOBILNYCH

Opracuj politykę określającą które usługi są dostępne dla poszczególnych typów urządzeń

Przygotuj politykę określającą jakie usługi powinny być dostępne dla poszczególnych typów urządzeń. Przy tworzeniu takiej polityki trzeba wziąć pod uwagę:

- zagrożenia związane z danym typem urządzeń,
- zagrożenia związane z miejscem, w którym urządzenia będą wykorzystywane,
- konsekwencje wykradzenia danych z danej usługi,
- konsekwencje uzyskania przez osoby nieuprawnione dostępu do danej usługi.

Przykładowo polityka może być zbudowana w następujący sposób:

- firmowe urządzenia mobilne, zarządzane i zabezpieczone przez dział IT, połączone przez VPN mają dostęp do wszystkich usług.
- firmowe urządzenia mobilne, zarządzane i zabezpieczone przez dział IT, połączone bez VPN mają dostęp tylko do usług X, Y, Z.
- prywatne komputery mobilne pracowników spełniające odpowiednie wymagania bezpieczeństwa (np. szyfrowanie dysku) mają dostęp tylko do usług X, Y.
- inne prywatne urządzenia mobilne (telefony, tablety) pracowników mają dostęp tylko do podstawowych usług z niskim ryzykiem, np. webowego klienta mailowego.

WYJAŚNIENIE

Tak skonstruowana polityka pozwala na ograniczenie potencjalnych strat wynikających z przejęcia któregoś urządzenia, zainfekowania go złośliwym oprogramowaniem czy ataku man in the middle (patrz Poradnik techniczny: Man in the middle).

09

BEZPIECZEŃSTWO PRACY ZDALNEJ I URZĄDZEŃ MOBILNYCH

Ustal politykę dotyczącą szyfrowania dysków i nośników danych

Jeśli na jakichś urządzeniach (np. laptopy, telefonu, dyski zewnętrzne) znajdują się wrażliwe i istotne dla biznesu dane to wdróż politykę pełnego szyfrowania tych dysków i nośników danych.

WYJAŚNIENIE

Szyfrowanie znacznie zmniejsza ryzyko uzyskania nieautoryzowanego dostępu do danych, np. w przypadku kradzieży laptopa.

Przygotuj procedury postępowania w przypadku zgubienia lub kradzieży urządzenia

Przygotowane procedury powinny obejmować:
Pożądane zachowanie użytkownika w momencie odkrycia faktu zagubienia lub kradzieży – zazwyczaj zgłoszenie do odpowiedniej osoby lub działu IT.

Informacje, które powinien dostarczyć użytkownik urządzenia – jakie dane były na urządzeniu, w jakim stanie było urządzenie (wyłączone, wylogowane, zalogowane) oraz jakie były okoliczności zdarzenia.

Działania do wykonania przez dział IT mające na celu redukcję ryzyka i potencjalnych strat – np. odebranie uprawnień kontom ze skradzionego urządzenia, zablokowanie dostępu do usług, zdalne wyczyszczenie dysku, próba lokalizacji urządzenia, zgłoszenie na policję.

WYJAŚNIENIE

Sytuacja zgubienia lub kradzieży urządzenia zawierającego firmowe dane lub umożliwiającego dostęp do firmowych usług może być poważnym zagrożeniem dla działania firmy. Z tego względu potrzebna jest jak najszybsza i jak najbardziej skuteczna reakcja. Przygotowane procedury mogą znacząco przyspieszyć cały proces.

10

ZABEZPIECZENIE DANYCH

Ustal politykę tworzenia kopii zapasowych

Opracuj politykę określającą następujące elementy:

- Jakie dane powinny być objęte tworzeniem kopii zapasowych – w tym punkcie potrzebne jest zidentyfikowanie danych, które są ważne dla firmy i powinny być objęte tworzeniem kopii zapasowych.
- Jak często powinny być tworzone kopie zapasowe – w tym punkcie potrzebne jest określenie jak często powinny być tworzone kopie zapasowe danych zidentyfikowanych.
- W poprzednim punkcie. Dane można podzielić na kilka kategorii, a następnie określić częstotliwość dla poszczególnych kategorii. Częstotliwość tworzenia kopii zapasowych powinna zależeć od tego na utratę danych.
- Z jakiego czasu może pozwolić sobie firma.
- Ile kopii powinno być tworzonych – jeśli dane są przechowywane tylko w jednym egzemplarzu to mogą zostać bardzo łatwo utracone. Dane docelowo powinny być przechowywane w przynajmniej 3 egzemplarzach, z zastosowaniem strategii 3-2-1.

WYJAŚNIENIE

Strategia 3-2-1 oznacza posiadanie przynajmniej 3 kopii danych:

1. Dane przechowywane lokalnie, na urządzeniach użytkowników.
2. Lokalna kopia zapasowa – umożliwia ona szybkie odzyskanie danych w razie awarii 1.
3. Kopia zapasowa w zewnętrznej lokalizacji – umiejscowienie kopii danych w zewnętrznej lokalizacji zabezpiecza firmę w sytuacji jednoczesnego zniszczenia danych z punktu 1 i 2 (np. w wyniku pożaru siedziby firmy). Jeśli do zewnętrznej kopii wykorzystywana jest technologia chmurowa to trzeba zwrócić uwagę na politykę przechowywania danych w chmurze.

Jeśli dane przechowujemy tylko w chmurze, nie na urządzeniach użytkowników, to trzeba zweryfikować czy firma dostarczająca dane rozwiązanie chmurowe tworzy i przechowuje kopie zapasowe zgodnie z wymaganiami firmy (liczba kopii, różne lokalizacje, czas ewentualnego odtworzenia danych).

11

ZABEZPIECZENIE DANYCH

Ustal politykę przechowywania danych w chmurze

Ustal politykę określającą jakie dane mogę być przechowywane w poszczególnych rozwiązaniach chmurowych. Polityka powinna być zbudowana z uwzględnieniem:

- prawnych aspektów określających gdzie powinny być przechowywane dane (np. część danych musi być przechowywana na terenie Unii Europejskiej),
- prawnych aspektów danego rozwiązania chmurowego (kto ma dostęp do przechowywanych w chmurze danych, w jakich sytuacjach mogą zostać udostępnione stronie trzeciej, np. policji),
- poziomu bezpieczeństwa dostarczanego przez dane rozwiązanie chmurowe (można np. zweryfikować czy zdarzały się już z niej wycieki, czy dane są szyfrowane na dyskach i podczas przesyłu, itd).

WYJAŚNIENIE

Opracowana polityka pozwoli na świadome używanie rozwiązań chmurowych oraz uniknięcie ewentualnych problemów prawnych i incydentów.

12

ZABEZPIECZENIE DANYCH

Ustal procedury postępowania z zużytymi/niepotrzebnymi nośnikami danych

Procedury powinny zostać przygotowane przy udziale administratorów i obejmować informacje:

- jakie nośniki są niszczone,
- w jaki sposób nośniki danych są czyszczone i niszczone,
- gdzie zniszczone nośniki są przekazywane.

WYJAŚNIENIE

Opracowane procedury pomogą uniknąć wycieków danych spowodowanych przez wyrzucenie nośników bez uprzedniego wyczyszczenia ich przez administratorów.

Ustal politykę dostępu do danych

Przygotuj politykę określającą które osoby mogą mieć dostęp do jakich danych i w jaki sposób. Przykładowo:

Do danych finansowych dostęp mają:
- prezes z komputera firmowego oraz z firmowego mobilnego laptopa,
- księgowa z komputera firmowego.

Przygotowanie takiej polityki wymaga:

1. Kategoryzacji danych firmowych.
2. Określenia dla każdej kategorii kto powinien mieć do niej dostęp.
3. Określenia dla każdej osoby posiadającej dostęp do danej kategorii z jakich urządzeń może do tych danych się dostać.

WYJAŚNIENIE

Opracowana polityka zmniejszy ryzyko wycieku danych, a w razie ewentualnego incydentu będzie łatwiej ustalić źródło wycieku.

13

ZABEZPIECZENIE USŁUG INTERNETOWYCH I OCHRONA INFRASTRUKTURY SIECIOWEJ / RUCHU SIECIOWEGO

Ustal politykę dostępu do usług

Podobnie jak w punkcie: “Ustal politykę dostępu do danych”, podobna procedura powinna zostać wykonana dla usług firmowych. Trzeba określić które osoby mogą mieć dostęp do jakich usług i w jaki sposób, przykłady:

Do usługi zgłaszania urlopu ma dostęp:
- każdy pracownik z dowolnego urządzenia.

Do usług księgowych ma dostęp:
- każdy pracownik działu finansowego z firmowych urządzeń znajdujących się w sieci firmy.

WYJAŚNIENIE

Opracowana polityka zmniejszy ryzyko wycieku lub nieautoryzowanej zmiany danych, a w razie ewentualnego incydentu ułatwi postępowanie powłamaniowe.

Ta polityka jest ściśle związana z polityką dostępu do danych (Zabezpieczenie danych) oraz z polityką określającą które usługi są dostępne dla poszczególnych typów urządzeń (Bezpieczeństwo pracy zdalnej).

14 ZABEZPIECZENIE USŁUG INTERNETOWYCH I OCHRONA INFRASTRUKTURY SIECIOWEJ / RUCHU SIECIOWEGO

Zadbaj o stworzenie osobnej sieci dla urządzeń prywatnych pracowników i gości

Jeżeli część firmowych usług lub danych jest dostępna tylko z wewnętrznej sieci firmowej to warto rozważyć utworzenie osobnej sieci dla urządzeń innych niż firmowe.

WYJAŚNIENIE

Łączenie się prywatnych urządzeń pracowników lub gości do wewnętrznej sieci firmy niesie za sobą duże ryzyko, ponieważ te urządzenia niekoniecznie są zabezpieczone tak dobrze jak urządzenia firmowe. Istnieje również ryzyko, że atakujący będzie udawał “gościa” firmy. Połączenia z tej osobnej sieci powinny być traktowane jak połączenia z zewnątrz firmy.

Ta polityka jest ściśle związana z polityką dostępu do danych (Zabezpieczenie danych) oraz z polityką określającą które usługi są dostępne dla poszczególnych typów urządzeń (Bezpieczeństwo pracy zdalnej).

15

INNE

Okresowo przeprowadzaj testy penetracyjne

Poziom zabezpieczeń infrastruktury i świadomości pracowników należy co jakiś czas badać. Testy penetracyjne, zlecone firmie zewnętrznej, są tylko jedną z możliwości i należy traktować je jako jedną z możliwości. Ważne jest, aby metoda badania testowała rzeczywiste bezpieczeństwo i świadomość a nie tylko ich odwzorowanie w dokumentach.

16

OCHRONA POCZTY ELEKTRONICZNEJ

Ustal politykę bezpieczeństwa informacji przesyłanych drogą elektroniczną

Opracuj politykę określającą sposób przesyłania poszczególnych informacji drogą elektroniczną, ze szczególnych uwzględnieniem informacji szczególnie istotnych dla Twojego przedsiębiorstwa (tajemnica przedsiębiorstwa), danych osobowych itp. W przypadku danych szczególnie istotnych wykorzystaj dodatkowe metody zabezpieczenia przed wyciekiem danych (patrz: Zadbaj o szyfrowanie wiadomości i załączników).

WYJAŚNIENIE

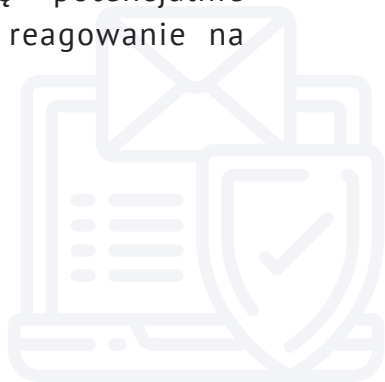
Kategoryzacja informacji oraz określenie reguł ich przesyłania drogą elektroniczną spowoduje, że pracownicy będą mieli jasne procedury, które określą w których przypadkach należy stosować dodatkowe zabezpieczenia chroniące przed wyciekiem danych lub potencjalną kradzieżą.

Przygotuj procedurę reagowania na podejrzane wiadomości

Pracuj procedurę, dzięki której pracownicy będą wiedzieć w jaki sposób powinni zareagować na podejrzane wiadomości i do kogo zgłaszać takie incydenty.

WYJAŚNIENIE

Przygotowana procedura sprawi, że dla Twoich pracowników będzie jasne w jaki sposób powinni się zachować po otrzymaniu podejrzanej wiadomości. Zmniejszy to liczbę potencjalnie groźnych sytuacji oraz umożliwi efektywniejsze reagowanie na incydenty bezpieczeństwa.



POLSKA PLATFORMA
BEZPIECZEŃSTWA WEWNĘTRZNEGO

Polska Platforma Bezpieczeństwa Wewnętrznego

ul. Słowackiego 17/11
60-822 Poznań
www.ppbw.pl
tel.: (61) 663 02 21
e-mail: standard-cyber@ppbw.pl

Fundusze Europejskie Inteligentny Rozwój
Rzeczpospolita Polska
Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Projekt pt.: „Cyberbezpieczeństwo – standard PPBW dla MŚP i instytucji publicznych" współfinansowany ze środków Unii Europejskiej.