STÓJ | POMYŚL | POŁĄCZ

Lista kontrolna technologii w biznesie

Firmy nieprzerwanie wdrażają i wykorzystują nowe technologie. Różnorodne rozwiązania wymagają odrębnego podejścia w zakresie zarządzania ryzykiem i zapewniania bezpieczeństwa. Poniższa lista została przygotowana, aby pomóc zidentyfikować w Twojej firmie obszary wymagające szczególnej ochrony. Zawiera także porady i zalecenia pomocne przy zapobieganiu, wykrywaniu i reagowaniu na incydenty w cyfrowym świecie.

☐ WI-FI	☐ WSPÓŁDZIELENIE PLIKÓW	☐ USB
☐ ROUTERY	☐ DRUKARKI/KOPIARKI/FAKSY	☐ STRONA WWW
☐ FIREWALLE	☐ USŁUGI CHMUROWE	☐ SIECI SPOŁECZNOŚCIOWE
☐ URZĄDZENIA MOBILNE	☐ VPN	☐ TERMINALE POS
☐ E-MAIL	☐ INTERNET RZECZY	☐ DOSTAWCY ZEWNĘTRZNI

STÓJ | POMYŚL | POŁĄCZ

Lista kontrolna technologii w biznesie

Wi-Fi

- ☐ Korzystaj z silnych haseł dla konta administratora oraz dostępu do sieci.
- ☐ Używaj bezpiecznego szyfrowania (WPA2 + AES lub WPA3).
- ☐ Przygotuj wydzieloną sieć dla gości.
- ☐ Zadbaj o fizyczne bezpieczeństwo urządzeń sieciowych.
- ☐ Miej ograniczone zaufanie do hotspotów Wi-Fi. Unikaj dostępu do informacji wrażliwych w ogólnodostępnych sieciach. W sieciach publicznych korzystaj z połączenia VPN.

Współdzielenie plików

- ☐ Ogranicz zakres lokalizacji, z których możliwe jest uzyskanie dostępu do danych wrażliwych.
- ☐ Tam, gdzie to możliwe, korzystaj z oprogramowania szyfrującego.
- ☐ Pracując z plikami, stosuj nazewnictwo zmniejszające prawdopodobieństwo wyjawienia rodzaju informacji, jakie zawierają.
- ☐ Monitoruj sieć pod kątem informacji wrażliwych - możesz to robić samodzielnie lub korzystać z zewnętrznego usługodawcy.
- ☐ Darmowe rozwiązania często nie zapewniają ochrony prawnej na poziomie odpowiednim dla biznesu.

Urządzenia USB

- ☐ Przed użyciem, skanuj nośniki wymienne pod kątem wirusów i złośliwego oprogramowania.
- ☐ Korzystaj wyłącznie z urządzeń USB dopuszczonych do użytku na terenie firmy.
- ☐ Zadbaj o szkolenia pracowników w zakresie profilaktyki incydentów z użyciem urządzeń USB.

Routery i przełączniki

- ☐ Korzystaj z rozwiązań monitorujących ruch sieciowy, zwracaj uwagę na anomalie.
- ☐ Ogranicz zdalny dostęp do interfejsów administracyjnych.
- ☐ Pamiętaj o wylogowaniu się z urządzenia po zakończeniu zmian w konfiguracji.
- ☐ Dbaj o aktualizacje oprogramowania na urządzeniach.
- ☐ Używaj bezpiecznych haseł.

Drukarki/Kopiarki/Faksy

- ☐ Bądź świadomy, że drukarki, kopiarki i faksy to także komputery.
- ☐ Wybieraj urządzenia, które posiadają możliwości szyfrowania i bezpiecznego usuwania danych.
- ☐ Korzystaj z oferowanych przez urządzenie funkcjonalności w zakresie bezpieczeństwa.
- ☐ Zabezpiecz/zniszcz bezpiecznie przechowywane na urządzeniu dane, przed przekazaniem go do utylizacji.
- ☐ Zmień domyślne hasło i wyłącz możliwość bezpośredniego logowania do urządzenia z sieci zewnętrznych.

STÓJ | POMYŚL | POŁĄCZ

Lista kontrolna technologii w biznesie

Strona WWW

- ☐ Pamiętaj o aktualizacjach bezpieczeństwa i aktualnym oprogramowaniu na serwerze.
- ☐ Sam również korzystaj z aktualnego oprogramowania.
- ☐ Wymagaj od użytkowników stosowania bezpiecznych haseł w celu zalogowania się do witryny.
- ☐ Ogranicz możliwość przesyłania plików bezpośrednio na serwer.
- ☐ Rozważ możliwość przeprowadzenia testów bezpieczeństwa witryny.
- ☐ Zarejestruj nazwy domenowe brzmiące podobnie do adresu Twojej strony WWW.

Firewalle

- ☐ Skonfiguruj reguły blokujące ruch, który nie jest konieczny dla Twojej firmy.

Usługi chmurowe i dostawcy zewnętrzni

- ☐ Przedyskutujcie z podmiotami trzecimi politykę bezpieczeństwa, postarajcie się utrwalić ją w formie umowy lub kontraktu.

Sieci społecznościowe

- ☐ Przygotuj politykę zarządzania stronami na portalach społecznościowych, wydziel role dla redaktorów.
- ☐ Ogranicz dostęp administracyjny.
- ☐ Wymagaj dwuskładnikowego uwierzytelniania.
- ☐ Zadbaj o bezpieczeństwo urządzeń mobilnych.

Urządzenia mobilne

- ☐ Zadbaj o aktualizacje oprogramowania.
- ☐ Odinstaluj nieużywane aplikacje.
- ☐ Zabezpiecz urządzenia za pomocą hasła lub innego bezpiecznego rozwiązania (skorzystaj np. z czytnika odcisku palca). Przechowuj urządzenia w bezpiecznym miejscu.
- ☐ Zaszyfruj dane wrażliwe.
- ☐ Upewnij się, że funkcje umożliwiające zdalne zlokalizowanie i usunięcie zawartości urządzenia są aktywne.

VPN (Wirtualne Sieci Prywatne)

- ☐ Używaj silnych haseł, bezpiecznych rozwiązań uwierzytelniających oraz szyfrowania.
- ☐ Dostęp do usługi ogranicz do osób, które rzeczywiście go potrzebują.
- ☐ Zadbaj o ochronę antywirusową użytkowników.

STÓJ | POMYŚL | POŁĄCZ

Lista kontrolna technologii w biznesie

Terminale POS

- ☐ Korzystaj z niepowtarzalnego, trudnego do złamania hasła. Zmieniaj je w razie potrzeby.
- ☐ Wydziel konto administratora i konta dla zwykłych użytkowników.
- ☐ Zadbaj o bezpieczeństwo swoich urządzeń - pamiętaj o aktualizacjach oprogramowania.
- ☐ Unikaj przeglądania Internetu na terminalach POS.
- ☐ Korzystaj z ochrony antywirusowej.

E-mail

- ☐ Usuwaj wiadomości, które budzą Twoje podejrzenia. Zachęcaj współpracowników do informowania o podejrzanych wiadomościach.
- ☐ Zapewnij odbiorcom Twoich wiadomości możliwość wypisania się z listy dystrybucyjnej.
- ☐ Zadbaj o stosowanie bezpiecznych i niepowtarzalnych haseł w miejscu pracy.
- ☐ Aktywuj dwuskładnikowe uwierzytelnianie.

Internet rzeczy

- ☐ Wydziel osobną, chronioną sieć dla urządzeń IoT, pamiętaj o zmianie domyślnych haseł.
- ☐ Dowiedz się, jakie informacje przetwarzają Twoje urządzenia. Zweryfikuj w jaki sposób są zabezpieczone oraz przechowywane.
- ☐ Rozważ, czy urządzenia IoT są właściwym rozwiązaniem do dedykowanych im zadań.
- ☐ Wybieraj urządzenia od producentów z udokumentowaną historią dostarczania bezpiecznych urządzeń IoT.
- ☐ Tam gdzie to możliwe, instaluj aktualizacje bezpieczeństwa.

DODATKOWE WSKAZÓWKI

Bezpieczna utylizacja

- ☐ Wiele urządzeń (nie tylko komputery i telefony) posiada wewnętrzną pamięć. Pamiętaj o bezpiecznym usunięciu danych, przed przekazaniem urządzenia dalej.

(Źródło: www.ic3.gov).

Odwiedź https://stojpomyslpolacz.pl i dowiedz się więcej.