Najlepsze praktyki w zakresie bezpieczeństwa

Poniższe kwestie i powszechne obawy są nieodłączną częścią dzisiejszego świata połączonych urządzeń. Świadomość ich istnienia to pierwszy krok. Następnym krokiem jest zastosowanie tych opartych na zdrowym rozsądku najlepszych praktyk w stosunku do wszystkich swoich połączonych urządzeń. Niniejszej listy kontrolnej można używać jako przewodnika pomagającego zaplanować działania.

1. Rozpocznij wcześnie

Planuj dla nowych technologii, które chcesz wdrożyć, uwzględniając sposoby ich chronienia.

2. Chroń dane

Tam, gdzie to możliwe, korzystaj z połączeń szyfrowanych i uwierzytelnianych.

3. Kontroluj usługi

Rozważ wyłączenie tych usług, z których korzystania nie planujesz.

4. Zmień hasła

Korzystanie z haseł domyślnych ułatwia hakerom dostęp do urządzeń. **Włącz hasła dostępu do interfejsów użytkownika.**

5. Zarządzanie zdalne

Wykorzystaj zalety bezpiecznego zdalnego systemu zarządzania, który umożliwi Ci szybkie aktualizowanie ustawień. Im dłużej urządzenia, rozwiązania i systemy korzystają z przestarzałych ustawień, tym łatwiejszym celem ataku się stają.

6. Włącz funkcję dziennika aktywności

Jeżeli dostępne są dzienniki aktywności i kontroli, korzystaj z nich w celu wykrywania niewłaściwego zachowania.

7. Kontroluj dostęp do informacji

Harmonogramy i plany aktualizacji udostępniaj wyłącznie tym pracownikom, którym są one niezbędne. Kiedy plany aktualizacji zna zbyt duża liczba pracowników, zwiększa się ryzyko naruszeń bezpieczeństwa.

8. Monitoruj rozłączone urządzenia

Opracuj metodę stałego monitorowania swojego systemu pod kątem rozłączonych urządzeń. W razie podejrzeń, że dane urządzenie zostało usunięte, wycofaj jego dane uwierzytelniające do chwili, aż będziesz w stanie potwierdzić jego lokalizację.

9. Możliwość aktualizowania

Wybieraj urządzenia, które można aktualizować przez cały długi czas ich eksploatacji, aby pozostawać na bieżąco z nowymi standardami. Dbaj o to, aby Twoje systemy były w stanie zapobiegać ingerencji w pliki aktualizacyjne.

10. Prawidłowo wycofuj urządzenia z użytku

Planuj wycofywanie urządzeń z użytku poprzez usuwanie ustawień systemów firmowych, usuwanie kont/danych uwierzytelniających użytkowników i sprawdzanie, czy istniejące systemy nie zostały na stałe zaprogramowane na szukanie wycofanych egzemplarzy.

11. P.I.D.

Na wszystkich etapach cyklu życia urządzenia **uwzględniaj kwestie poufności (P), integralności (I) i dostępności (D).**

12. Nieustannie planuj

Uaktualnianie praktyk w zakresie bezpieczeństwa powinno być stałym priorytetem. Planowanie bezpieczeństwa to nie jednorazowe wydarzenie.

Czy wiesz, że...?

360.000 USD

Szyfrowanie zmniejsza koszty naruszenia bezpieczeństwa danych średnio o **360.000 USD**, co czyni je najskuteczniejszym środkiem zaradczym przeciwko włamaniom przez hakerów.[1]

81%

Przyczyną **81%** przypadków naruszenia bezpieczeństwa danych poprzez włamania przez hakerów było wykorzystanie skradzionych lub słabych haseł.[2]

1,2 mln USD

Firmy, które dysponują zespołami ds. reakcji na incydenty związane z naruszeniem bezpieczeństwa danych i testują plany takich reakcji, obniżają koszty powodowane przez naruszenie o ponad **1,2 mln USD.**[3]

38%

Incydenty związane z bezpieczeństwem z udziałem urządzeń klasy korporacyjnej zgłosiło **38% firm**.[4]

40%

40% respondentów twierdzi, że cyberataki to czynnik zwiększający znaczenie zabezpieczania urządzeń mobilnych.

197 dni

Zorientowanie się, że doszło do naruszenia bezpieczeństwa danych zajmuje organizacjom średnio 197 dni.[5]

[1] „Cost of a Data Breach Report 2019", IBM Security • [2] „2017 Verizon Data Breach Investigations Report", IBM Security • [3] „Cost of a Data Breach Report 2019" • [4] „Carbon Black Incident Response Threat Report", listopad 2018 r. • [5] Badanie „Cost of Data Breach" z roku 2018 i 2019, Ponemon Institute