Best practice per la sicurezza

Considerazioni e problematiche comuni strettamente associate al mondo digitale di oggi popolato da dispositivi interconnessi. La consapevolezza è il primo passo. Quello successivo è l'applicazione di queste best practice di buonsenso a tutti i vostri dispositivi connessi. Usate questa lista come guida per la pianificazione.

1. Iniziare da subito

Pianificate le tecnologie da introdurre e pensate a come proteggerle.

2. Proteggere i dati

Usate connessioni crittografate e autenticate quando possibile.

3. Controllare i servizi

Valutate la possibilità di disattivare i servizi tecnologici che prevedete di non utilizzare.

4. Cambiare le password

Le password predefinite rendono più semplice l'accesso ai dispositivi per gli hacker. **Impostate delle password per l'accesso all'interfaccia utente.**

5. Gestione remota

Avvaletevi di un sistema di gestione remota protetto per aggiornare rapidamente le impostazioni. Quanto più a lungo dispositivi, soluzioni e sistemi usano impostazioni obsolete, più diventano facili obiettivi di possibili attacchi.

6. Registrazione delle attività

Usate registri delle attività e di audit quando possibile per scoprire comportamenti anomali e dannosi.

7. Confidenzialità

Mettete al corrente di programmi e piani solo le persone direttamente coinvolte. Se troppi dipendenti conoscono queste informazioni, le probabilità di violazioni della sicurezza aumentano.

8. Monitorare i dispositivi OOT

Sviluppate un metodo per monitorare costantemente il sistema al fine di individuare i dispositivi che hanno perso contatto ("out-of-touch"). Se sospettate che un dispositivo sia stato rimosso, ritirate le sue credenziali finché non siete in grado di verificarne la posizione.

9. Aggiornabilità

Scegliete i dispositivi che possono essere aggiornati nel corso della loro vita operativa per mantenerli al passo con i nuovi standard. Assicuratevi che i sistemi di aggiornamento impediscano la manomissione dei file di aggiornamento.

10. Ritiro dei dispositivi

Pianificate il ritiro dei dispositivi rimuovendo le impostazioni dei sistemi aziendali, cancellando gli account e le credenziali degli utenti dei dispositivi e verificando che i sistemi esistenti non siano codificati in modo permanente per la ricerca delle unità ritirate.

11. C.I.D.

Valutate sempre i fattori "Confidenzialità", "Integrità" e "Disponibilità" durante tutte le fasi del ciclo di vita dei dispositivi.

12. Pianificazione continua

Gli aggiornamenti delle politiche in materia di sicurezza devono rimanere una priorità costante. La pianificazione della sicurezza non è un evento una tantum.

Lo sapevate?

360.000 $

La crittografia riduce al minimo i costi delle violazioni di dati, mediamente per un importo di **360.000 $**, ed è la contromisura più efficace contro gli hacker.[1]

81%

L'uso di password rubate o troppo deboli è associato all'**81%** delle violazioni di dati da parte di hacker.[2]

1,2 milioni di dollari

Le aziende che dispongono di team di pronto intervento e testano piani di risposta riducono il costo di una violazione di oltre **1,2 milioni di dollari.**[3]

38%

Il **38%** delle aziende ha registrato problemi di sicurezza che hanno coinvolto i dispositivi aziendali.[4]

40%

Secondo il **40%**, gli attacchi informatici sono un fenomeno che sta rendendo sempre più importante la protezione dei dispositivi mobili.

197 giorni

Un'azienda ha bisogno mediamente di 197 giorni per scoprire una violazione di dati.[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, November 2018 • [5] 2018 and 2019 Cost of Data Breach, Ponemon Institute