10 mikilvæg atriði til að vernda fyrirtækið þitt gegn tölvuárásum

TÖLVUAÐSTOÐ

www.tolvuadstod.is - Stórhöfði 17 - 5 500 200

1. Öruggar innskráningar án lykilorða

Flestar tölvuárásir hefjast með stuldi eða ágiskun á lykilorð. Við mælum með að innleiða lykilorðalausar innskráningar þar sem það er mögulegt. Að lágmarki ætti þó að virkja tveggja þátta auðkenningu og notast við sterk lykilorð.

2. Aðgangsstýring og lokun notendaaðganga

Of mikil aðgangsréttindi og óvirkir notendur eru öryggisáhætta. Gæta þarf þess að aðgangur sé í samræmi við rétt hlutverk og að aðgangi sé lokað eða breytt um leið og notendur hætta eða breyta um hlutverk.

3. Örugg afritun og endurheimt gagna

Afritun er síðasta vígið. Það er algengur misskilningur að það sé óþarfi að afrita skýjaþjónustur eins og Microsoft 365 og Google Workspace. Örugg afrit ættu að vera geymd hjá þriðja aðila, þar sem gögnin eru óbreytanleg eftir afritun. Mikilvægt er að prófa endurheimt gagna reglulega.

4. Reglulegar uppfærslur á hugbúnaði og stýrikerfum

Uppfærslur lagfæra þekkta öryggisgalla sem árásaraðilar nýta sér. Tryggja þarf að stýrikerfi, forrit, netbúnaður, smáforrit og afritunarkerfi séu uppfærð með reglulegu millibili.

5. Fræðsla og meðvitund starfsmanna

Öryggisbrot má oft rekja til mannlegra mistaka. Regluleg fræðsla um netöryggi, svikapósta, vefveiðar og hlekkjasvindl eykur meðvitund og dregur úr áhættu.

6. Tölvupóstöryggi og sannvottun léna

Nauðsynlegt er að stýring á léni og nafnaþjóni sé á höndum fárra aðila. Gott er að velja einn til tvo aðila innanhús eða öruggan þjónustuaðila sem sér um breytingar og viðhald. Þetta er til þess að halda pósti og lénaauðkenningum í lagi, vernda gegn fölsuðum póstum og tryggja að samskiptin séu ekki hleruð eða fölsuð í tölvupóstum sem og á vefsvæði.

7. Yfirsýn yfir tæki og forrit

Tryggja þarf yfirsýn yfir öll tæki, hugbúnað og (smá)forrit sem starfsmenn nota í tengslum við vinnu. Óskráð eða ósamþykkt tæki og smáforrit geta valdið alvarlegum öryggisbrestum.

8. Vörn gegn spilliforritum og árásum

Mikilvægt er að vernda tölvur og skýjaumhverfi með rauntímagreiningu og sjálfvirkri svörun. Endabúnaðarvörn og samþætt öryggisvörn greina óvenjulega virkni á tölvum og netbúnaði og stöðva flóknar árásir sem komast fram hjá hefðbundnum vírusvörnum.

9. Stöðug vöktun og viðbragðsáætlun

Skilgreind vöktun og viðbragðsáætlun fyrir öryggisatvik eru lykilatriði til að tryggja að brugðist sé við á viðeigandi máta eftir alvarleika atvika.

10. Fylgstu með persónuvernd og öryggisskyldum

Flest fyrirtæki vinna með persónugreinanleg gögn og falla þar með undir persónuverndarlög (GDPR), sem krefjast öruggrar meðferðar gagna, þar með talið í pósthólfum og skjalageymslum. Einnig ber að huga að nýjum reglugerðum eins og NIS2 og DORA, sem krefjast aukins netöryggis og ábyrgðar. Brot gegn þessum reglum getur opnað fyrir árásir og leitt til alvarlegra viðurlaga og trúnaðarbrests.

Verndum **Vöktum** **Afritum**