

Nem tudja ellenőrizni az összes doménjét a Microsoft



A tengerentúli társaság számos aldoménnel rendelkezik, amelyek kezelése egyáltalán nem egyszerű feladat.

Michael Gaschet biztonsági kutató közölte, hogy az elmúlt időszakban nagyon sok problémás esetet jelzett a cégnek. Különösen a rosszul konfigurált DNS-bejegyzések száma nőtt meg az elmúlt három esztendő során. Egyes esetekben az ilyen hibák oda vezethetnek, hogy a támadók átvehetik az ellenőrzést az aldomének felett és azokkal visszaélhetnek, például kéréstlen vagy adathalász leveleket küldhetnek. A címzettek ebből csak azt észlelnék, hogy a Microsoft doménjéről érkezett az elektronikus postafiókjukba ilyen üzenet.

A szakember kiemelte, hogy az óriáscég illetékesei gyakran teljesen figyelmen kívül hagyták a jelzéseit, sőt, néhány esetben a problémákat gyakorlatilag inkább titokban kijavították, de csak a fontosabb aldomének, például a `cloud.microsoft.com` vagy az

`account.dpedge.microsoft.com` esetében. Gaschet rámutatott továbbá, hogy már 2017-ben elkészítette az első ilyen jellegű jelentését, amelyben az `msn.com` 21 aldoménjének hibás DNS-bejegyzéseiről tájékoztatta az amerikai vállalatot. A tavalyi anyagában már 142 esetről számolt be, akkor a `microsoft.com` aldoménjei voltak érintettek.

A biztonsági kutató szerint a Microsoft munkatársai csak a jelzések 5–10 százalékára reagáltak javításokkal. A hibák többsége a konfigurálások vagy a karbantartások során elkövetett gondatlanságra vezethető vissza. Előfordul, hogy az alkalmazottak egyszerűen nem veszik észre a betűhibákat és azok okoznak problémákat, de az is gyakori, hogy a DNS-bejegyzések olyan dolgokra utalnak, amelyek már régóta nem léteznek.

A jelenség egyébként nem új. Már 2014-ben is volt ilyen jellegű jelzés, de a kérdésben gyakorlatilag alig történt előrelépés. Ez elsősorban arra vezethető vissza, hogy eddig egyetlen támadó sem használta ki a kínákozó lehetőséget vagy egyszerűen nem vette észre a sebezhetőséget. Most viszont van egy kéréstlen elektronikus leveleket küldő csoport, amely a reklámjait a Microsoft egyik aldoménjét használva küldi el.

Forrás: <https://sq.hu/cikkek/it-tech/139960/nem-tudja-ellenorizni-az-osszes-domenjet-a-microsoft>

Válogatta: Berke Barnabásné