# **Southern Brokers**

# Cégleírás

Cégünk egy MNB által felügyelt befektetési vállalat, az alkalmazottaink a tőzsdén való kereskedéssel próbálják gyarapítani a befektető kliensek vagyonát. Mivel több százmilliós akár milliárdos összegekről van szó, elengedhetetlen, hogy folytonos, biztonságos hálózati hozzáférés legyen biztosítva a nálunk dolgozó kereskedőknek, mindazonáltal, hogy minden tranzakció valós időben történik az interneten, így akár pár perc leállás a rendszerben valakinek a vagyonát lenullázhatja.

# Redundáns kialakítás

A cég hálózatának tervezése közben minden olyan kritériummal számolnunk kellett, ami hibát, vagy leállást okozhat a rendszerben, hogy akár a véletlen tragédiaszerű, vagy megtervezett rosszindulatú események során is akadálymentesen folytatódhasson a kereskedelem. Ilyennek számít egy szolgáltatói leállás, vezeték meghibásodás, vagy akár belső rossz szándékú cselekmény. Ezek elkerülésének érdekében az elsődleges szerverünk egy bérelt adatközpontban helyezkedik el, konsant megfigyelés alatt áll, és monitorozva van minden hálózati forgalom. Itt az esedékes áramszüneteknél is biztosítva van a hálózat, szünetmentes áramellátással és tartalék agregátorokkal, és még számos kisebb terrorcselekmény ellen is védve van az épület. Mind ezek ellenére, az adaközpont meghibásodásának lehetősége nincs kizárva, ezért a cégünk saját telephelyén is kialakítottunk egy másodalagos szerverszobát, ami azonnal átvenné az összes üzemeltetési szerepkört a főszerver esetleges meghibásodásánál . A két telep folytonos szinkronizációt végez el egymás között, hogy minimálisra csökkenjen az adatvesztés lehetősége. Esetleges áramszünet miatt a saját telepünk is szünetmentes tápegységekkel vannak ellátva, illetve beszerltünk egy saját dízel aggregátort is, ami az épület minden esszenciális létesítményét el tudja látni árammal.

Biztonság, adatvédelem

Mivel a cégünk több száz ügyfél felettébb bizalmas adatait kezeli, tárolja, meg kell akadályoznunk minden adatszivárgási lehetőséget. Ennek érdekében a hálózatban semmi olyan apró rés nem keletkezhet, ami bármely fenyegetésnek kiteheti ezeket. A cél eléréshez fizikai és virtuális korlátozásokat kellett használnunk egyidejűleg. A cég belső hálózatát kívülről csak és kizárólag céges laptopokról és a Cisco AnyConnect VPN használatával lehet elérni, ami össze van kötve egy mobiltelefonos kétfaktoros hitelesítési rendszerrel. Ez önmagában kizárja azt a lehetőséget, hogy egy illetéktelen egy megfelelő felhasználónév és jelszó párosával beléphessen a belső hálózatunkba. A fő domain szervezeti egységei és felhasználói erősen korlátozott jogkörrel rendelkeznek, hogy ne tudjanak hozzáférni, vagy módosítani olyan fájlokat, amik az ügyfelek adatainak védelmét veszélyezteti. A céges számítógépeken minden idegen eredetű eszköz és alkalmazás futtatása le van tiltva. Minden olyan hozzáférési pont ami külső, vagy szolgáltatói hálózathoz csatlakozik egy nagy teljesítményű Cisco ASA tűzfallal van védve, ezzel fizikailag is megakadályozva a támadásokat. A vezeték nélüli vonalak fokozott sebezhetősége miatt a Wi-Fi hálózatunk nincs közvetlen összeköttetésbe a belső hálózattal.