Hírek

Közeledik az infoháborús világbajnokság újabb fordulója

Egy nemrég közzétett tanulmány pontokba szedve foglalja össze, hogy a digitális térben hányféle és milyen súlyos kihívást jelent a közelgő amerikai elnökválasztás biztosítása.

Most, hogy már tényleg csak hetek választanak el a 2020-as amerikai elnökválasztás tényleges megkezdésétől, az eddiginél is több figyelem irányul azokra a digitális kockázatokra, amelyek a legutóbbi, 2016-os esemény óta mindenki számára nyilvánvalók. A külföldi beavatkozási kísérletek nyomán az állami és szövetségi szervezetek a piaci szolgáltatókkal együtt készültek az új kihívásokra, és a kongresszus is 800 millió dollárral járult hozzá, hogy a választást a korábbinál jobban biztosítsák az egyes tagállamokban.

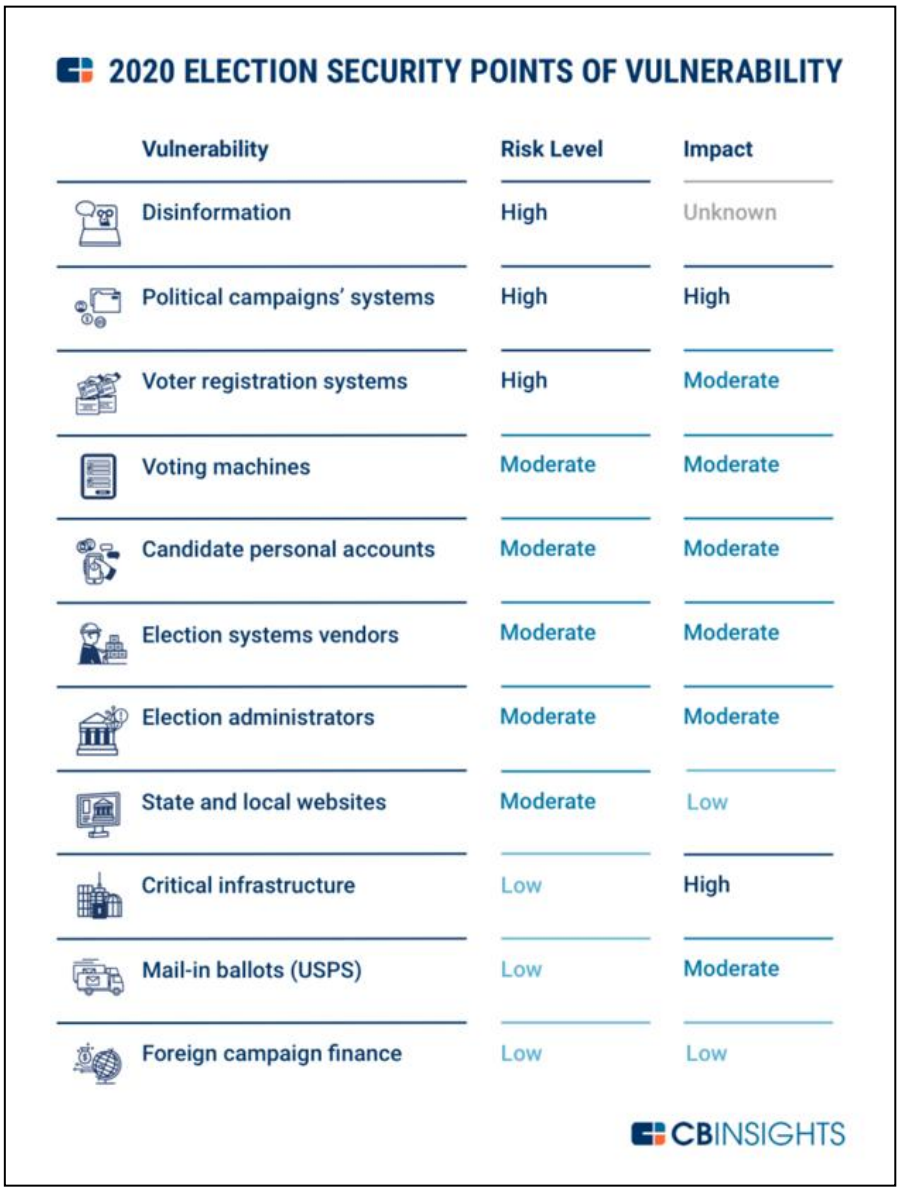
Bár a 2018-as félidős választásokra nem, a 2020-as megmérettetésre már lehetségesnek tartották a megfelelő felkészülést; ehhez mindenképpen szükségesnek látszott a megfelelő jogszabályokat megalkotása az online dezinformációval kapcsolatban, a megfelelő felelősségek tisztázása a szövetségi ügynökségeken belül, az egyes államok saját kapacitásainak kiépítése, legelsősorban pedig a az állampolgárok tudatosságának növelése, figyelembe véve a folyamatosan tapasztalható befolyásolási vagy beavatkozási kísérleteket.

Van, aminek még a következményei sem beláthatók

Legutóbb szeptember közepén számoltunk be a Microsoft közleményről, amelynek alapján az orosz, iráni és kínai állami háttérrel működő hekkercsoportok ismét ráálltak az amerikai elnökválasztásra, és sorozatos támadásokat intéznek a Trump vagy Biden kampányához köthető személyek és szervezetek email-fiókjai ellen. A sok száz támadás nagy részét a Microsoft szerint időben észlelték és blokkolták, de a jelenség teljesen egybevág azokkal a figyelmeztetésekkel, amelyeket az amerikai kormányügynökségek és a biztonsági cégek is időről időre kiadnak.

Hogy a felkészülés mennyire sikerült, azt csak az elkövetkező hetekben fogjuk megtapasztalni. Az mindenesetre valószínű, hogy – a Facebook korábbi biztonsági vezetőjének meghatározásával – a választások innentől kezdve valamiféle „infoháborús világbajnokságra” hasonlítanak majd. A CB Insights nemrég közzétett elemzésében összesen 11 pontban igyekezett azonosítani azokat a sebezhetőségeket, amelyek ebből a szempontból meghatározók lehetnek a választások lebonyolítására, figyelembe véve a kockázati tényezők súlyosságát és azok várható hatásait is.

A legmagasabb kockázati szintre a digitális csatornákon zajló dezinformációt, a kampánycsapatok informatikai hátterének sérülékenységét és a választói regisztrációs rendszert sorolták. Ezek közül a kis létszámú állandó munkatárssal és rengeteg, esetenként érzékeny információkhoz is hozzáférő önkéntessel dolgozó kampánystábok esetében nem csak a rizikót, de az incidensek várható következményeit is súlyosnak értékelték, míg az álhírek terjesztése volt az egyetlen olyan pont, ahol a hatásokat meg sem próbálták felbecsülni.



forrás: CB Insights – Countdown To The Election

Mindenre figyelni kell a jelöltektől a teljes rendszerekig

A kutatás az MIT médiaintézetének 2018-as tanulmányát idézi, amely szerint a dezinformáció sokkal hatékonyabban terjed: a legjobban menő álhírek akár 100 ezres nagyságrendben érhetik el a felhasználókat, míg a valós információra épülő tájékoztatás ennek a töredékéhez juttatható el. Mindez ellen technológiai szempontból a robotok és a deepfake tartalmak hatékonyabb felismerése, általában pedig a digitális média minőségének feltornázása lenne a megoldás – bár ezen a téren is sor került nyilvánvaló erőfeszítésekre, a helyzet az ideálistól még nagyon messze van.

A kampánycsapatok esetében a CB Insights azokat a kiberbiztonsági tanácsadó szolgáltatásokat emeli ki, amelyek nem hogy léteznek, de akár ingyenesen is igénybe vehetők, sőt esetenként kifejezetten gyártófüggetlen, direkt a választásokhoz kapcsolódó eszközökről van szó. A választói regisztráció problémája inkább műszaki jellegű, amennyiben nem könnyű feladat kizárni, hogy egy nagyszabású zsarolóvírus-kampány teljes adatbázisokat állítson a feje tetejére – itt nyilván sok múlik

a korai felismerésen és a backup megoldások alkalmazásán.

A közepes kockázatok között a CB Insights a szavazógépeket, a jelöltek személyes profiljait, a választási adminisztrációt, az állami és helyi weboldalakat, illetve a választási informatikai rendszerek gyártóit említi, de a ezek közül egyiket sem sorolja a legsúlyosabb következményeket hordozó fenyegetésekhez. A levélben való szavazásnál, a kampányok külföldi finanszírozásánál és a kritikus infrastruktúra védelménél már a kockázatokat is alacsonynak ítéli, bár utóbbi esetben nyilván olyan rendszerekről van szó, amelyek esetében minden diszrupció a legkomolyabb problémákat idézhetné elő.

A tanulmány publikus változatában az egyes szempontok bemutatásáról és a védekezés legfontosabb elemeiről itt lehet részletesebben olvasni.

Forrás: https://bitport.hu/kozeledik-az-infohaborus-vilagbajnoksag-ujabb-forduloja

Válogatta: Fonyó Istvánné