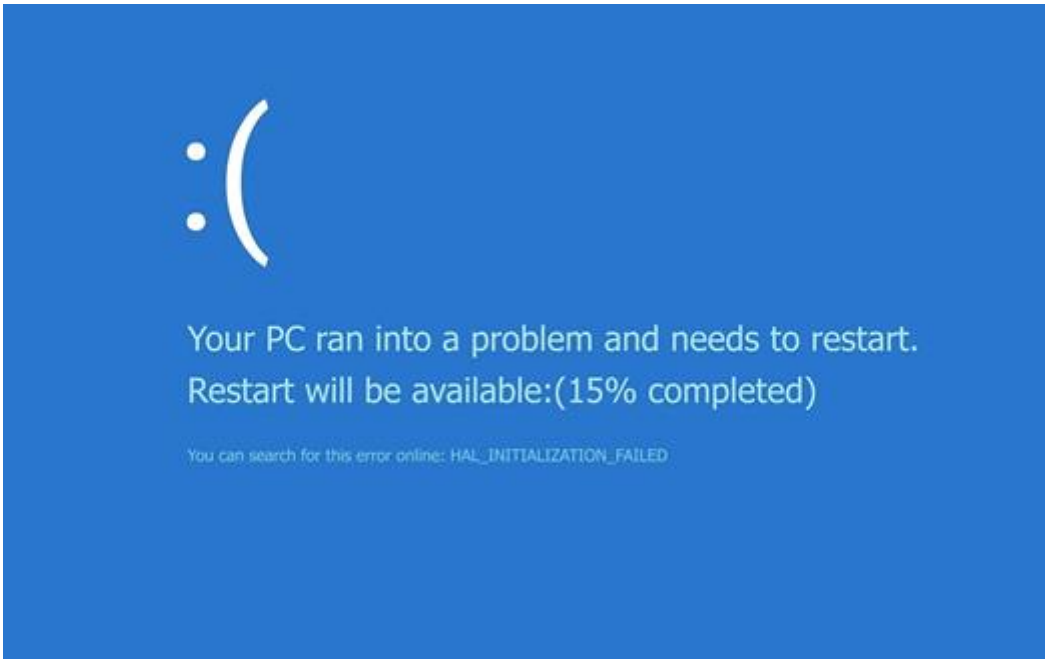
A Crowdstrike leállás margójára

Csizmazia-Darab István ⋮⋮ 2024. 07. 24.

Az elmúlt napok globális IT-piaci történéseit a Crowdstrike leállás és következményei uralták. Milyen tanulságok vonhatók le az esetből, és lehetünk-e, ha igen, hogyan felkészültebbek a jövőben? Vendégszerzőnk cikke ezekre a kérdésekre, felvetésekre (is) igyekszik választ adni.



Megáll az idő

A számítástechnika világában kevés ijesztőbb dolog létezik, mint amikor a Windows rendszeren megjelenik a kék halál képernyő (BSOD). A jelenség oka valamilyen végzetes rendszerhiba, amely leállásra kényszerítette a Windowst a további károk megelőzése érdekében.

A veszély még nagyobb, ha ezt egy nagyobb incidens részeként, tömeges szinten tapasztalják a felhasználók. Ilyenkor világszerte egyidőben rengeteg eszközt fagyhat le, és mindez képes jelentősen megzavarni a kritikus szolgáltatásokat, amelyeket nap mint nap igénybe veszünk.

Ezt tapasztalhattuk az elmúlt napokban. Többen elsőre kibertámadásra gyanakodtak, ám kiderült, nem egy Windows frissítés, hanem a CrowdStrike vírusvédelmi szoftver gyártója által kibocsátott hibás frissítés okozta világszerte a tömeges leállásokat.

A nagy informatikai összeomlás 8,5 millió Windows-eszközt érintett. Múlt csütörtök éjjel kezdődött, és péntek reggelre már számos helyen okozott lefagyást, kék halált.

Repterek, bankok, tévéadók, közlekedési terület, egészségügyi szektor, tőzsdék bénultak meg, emellett bezuhant a Crowdstrike részvények értéke is.

A legnevesebb biztonsági szakértők szerint is ez volt a történelem eddigi legnagyobb informatikai kiesése, sokan az ezredfordulón vártak ilyesmit az Y2K kapcsán, ami ott és akkor végül elmaradt.

A Crowdstrike jelentős szereplő a piacon, világszerte 20 ezer ügyfelük van, köztük a Fortune 500 listán szereplő vállalatok több mint fele, de az USA több jelentős kormányzati szervezete is a szoftverüket használja.

Ekkora világméretű leállást már régen láttunk. Sokan emlékezhetnek 2003-ban a Microsoft SQL szervereket támadó Slammer (más néven Zaphire) féregre, amely a nem frissített rendszerekben található biztonsági rést használta ki, és villámgyorsan terjedt tovább, ezzel pedig jelentős hálózati zavarokat, leállásokat okozott az interneten.

A megfertőződött SQL-szerverek 90%-a már a járvány első tíz percében áldozatul esett. Legalább 205 ezer gépre kerülhetett rá, és összességében pedig több mint 1 milliárd dolláros kárt okozott.

A vírusvédelem naprakész frissítése kulcsfontosságú volt már előzőleg is, de az antivírus gyártók által kibocsátott vírusismereti adatbázisok egyre sűrűbb és rövid reakcióidőkkel történő kiadása pont az ilyen incidensek hatására javult jelentősen.

Emellett sokakban akkoriban még nem tudatosult eléggé, hogy a vírusvédelem mellett a biztonsági frissítések futtatása is mennyire fontos. Itt ráadásul el is kerülhető lett volna az incidens, hiszen a kártevő által kihasznált sebezhetőséget befoltozó biztonsági hibajavító frissítést már 2002-ben, egy évvel korábban kibocsátotta a Microsoft.

Mi okozta a mostani problémát?

A szoftverfejlesztői munkában a megjelenés előtti szoftvertesztelés mindig is kulcsfontosságú volt, és manapság a globalizált üzleti világban kiemelt gondossággal kell ebben eljárni.

Sajnos, néha még a legszigorúbb szabályozottságú ellenőrzési folyamatoknál is előfordulhatnak problémák – szerencsére csak nagyon ritkán. A jelenlegi összetett IT-környezetben ez bármely IT-szállítóval megtörténhet, amelynek frissítenie kell a kritikus szoftvertermékeket.

Az ilyen eseteknél igyekeznek azonnal tájékoztatni az ügyfeleket, és a lehető legrövidebb időn belül soron kívüli javítást kibocsátani. Itt a frissítések gyakorisága lehetett az egyik fő oka, hogy a tesztelés nem szűrte ki a programozási hibát.

Az külön kiemelendő, hogy ilyen kritikus esetekben mind a szoftverfejlesztő cégek, mind a vírusvédelmi szakma is egységesen maximálisan segítőkész és együttműködő, minden lehetséges technikai segítséget, szakmai információt megadnak egymásnak, akár a konkurens gyártók részére is, amivel segíteni tudnak a probléma mielőbbi sikeres elhárításában.

Itt a megoldás végül az lett, hogy a gyártó kiadott egy javított frissítést, ám a helyreállítás így is nehézkes és időben hosszan elhúzódó folyamat volt.

A bűnözők is kihasználták az esemény utóéletét, és csaló leveleket küldtek a CrowdStrike Support nevével visszaélve, amelyekben kártékony weboldalakra mutató linkek, illetve rosszindulatú fájlmellékletek szerepeltek. Érdemes tehát erre is figyelni a közeljövőben.

Ennyire sérülékenyek vagyunk?

Az online felhasználók óriási száma (5,44 milliárd netező, Statista.com) és mai világunk hatalmas netes forgalma, informatikai beágyazottsága miatt a leállások mennyisége folyamatosan növekszik, és várhatóan nőni is fog az online felhasználók és a forgalom állandó növekedése miatt. Emiatt hirtelen sok millió ember válhat egy szolgáltatás-kimaradás áldozatává.

Esetünkben a Windows környezet elterjedtsége a világon hatalmas, a különféle alkalmazói szoftverek ügyfelei is rengeteg országból, sok vállalatból kerülnek ki, és mindenhol milliós, százmilliós méretű a felhasználói bázis.

Ahol az informatikai infrastruktúra nem sokféle, csekély a diverzitás, ott egyetlen műszaki incidens is globális szintű biztonsági problémákhoz, szolgáltatás kimaradásokhoz vezethet.

Ezt láthattuk, most például a repülésirányításnál is. Sok érintett szervezetnél látványosan hiányzott a vészhelyzeti terv, tovább súlyosbítva a helyzetet.

Sok idő kell a helyreállításhoz

A helyreállítás mindig időigényes, ez az informatikai rendszereknél is több napig tart, egyes területeken pedig, mint például a légiközlekedés, akár 8-10 napba is telhet, míg helyreáll a szokásos ügymenet.

Emlékezhetünk például, hogy 2024 áprilisában, mikor a heves esőzések miatt elöntötte a víz a dubai repteret, a kényszerleállás okozta torlódások után egy hétbe telt, mire a normál menetrendre vissza tudtak állni.

A leállások emellett képesek hatalmas veszteségeket is okozni. 2021 márciusában akadt el a 224 ezer tonnás, 400 méter hosszú Ever Given óriáshajó konténerekkel megpakolva a Szuezi-csatornán. Itt halad át a világ tengeri kereskedelmének 12%-a, a konténeres szállítás aránya viszont eléri a 30%-ot.

A baleset miatt több mint 300 hajó várakozott arra egy hétig, hogy átjusson, a leállás pedig napi 14-15 millió dollárba került a csatornának.

A több napos veszteglés a kereskedelemben és az ellátási láncokban pedig késéseket, áruhiányt és áremelkedéseket idézett elő.

Tartanunk kell a szoftverfrissítésektől?

Összességében elmondhatjuk, hogy napjainkban igen nagy részben már a szoftverek irányítják a világot. Köztudott, hogy a ki nem javított sebezhetőségek okozzák az adatvédelmi incidensek nagy részét. Tavaly összesen több mint 29 ezer biztonsági rést, sebezhetőséget jelentettek, szemben az egy évvel korábbi 25 ezerhez képest.

Minden alkalmazás frissítésre szorul, akárcsak az alapjául szolgáló operációs rendszer és firmware (az eszköz hardveréhez kapcsolódó speciális szoftvertípus).

A szoftverfrissítések amellett, hogy segítenek kivédeni a személyes és pénzügyi adatokat fenyegető veszélyeket, valamint számos problémát, hibát és hibás működést orvosolnak, új funkciókat tesznek elérhetővé, javítják a készülék akkumulátorának élettartamát és fokozzák a rendszer teljesítményét.

Ám ha ritkán is, de maguk a szoftverfrissítések is előidézhetnek problémákat, és semmi garancia nincs arra, hogy a későbbiekben ne forduljon elő hasonló eset.

A hibajavítások biztonságossága és előzetes tesztelése főképp a gyártó feladata, vállalati környezetben pedig bevett gyakorlat, hogy először tesztkörnyezetben frissítenek, és csak utána küldik ki a javításokat az éles gépekre.

A mostani incidens ellenére digitális életünk védelmének egyik leghatékonyabb eszköze továbbra is, ha napra készen tartjuk a szoftvereinket.

A szerző az ESET/Sicontact IT-biztonsági szakértője