NAGYOT ROBBANT A NYÍLT FORRÁSKÓDÚ, BIZTONSÁGI AKNA

Lelassul a vállalati innováció?

FORRÁS: 123RF.COM

Megingatta a nyílt forrású fejlesztési modellbe vetett bizalmat az évtized biztonsági eseményének kikiáltott Log4Shell-sérülékenység, ami lassíthatja a vállalati innovációt és a digitális fejlődést egyaránt. A szinte a fél világot működtető Java programozási nyelv sérülékenysége a vállalati patchelés bonyolultságára és biztonsági kihívásaira is felhívta a figyelmet.

Minecraft-rajongó fiaim december elején mutattak egy videót arról, hogy egy chat-felületen elküldött egyszerű szöveges üzenettel hogyan vették át egymástól a játékszervereket a vicces kedvű támadók. Akkor legyintettem egyet, mondván, ez biztos valami clickbait videó. Viszont pár nappal később megismertem a Log4j nevű naplózási keretrendszert, és hogy az hogyan ad az elkövetkező tíz évre munkát a biztonsági szakembereknek.

A megbízható megoldás volt a leggyengébb láncszem

A Log4j programozási rutinkészlet egy olyan, naplózáshoz használt eszköz, amelyet a Java-programozók 2001 óta használhatnak. A nyílt forráskódú megoldást bárki ingyen „levehette a polcról", és beépíthette a vállalati szoftverbe, az ügyfélszolgálati rendszerbe, a jegykezelő megoldásba – vagyis akármibe. A megoldás figyeli és naplózza a szoftver működését, megbízhatóan, kipróbáltan tette feladatát évtizedeken keresztül.

Amit a Java alapú Minecraft eredetileg a saját problémájának tartott, arról nagyon hamar kiderült, hogy az egész világot érinti. A szoftveres sérülékenységeket nyilvántartó Common Vulnerabilities and Exposures (CVE-) adatbázisban a „Log4-Shell" nevet nyert sérülékenység súlyossága 10-es besorolást kapott az 1-től 10-ig tartó skálán. A besorolást könnyű kihasználhatósága és népszerűsége támasztotta alá. Rengeteg vállalati szoftverbe, megoldásba beépítették, hosszú a listája az érintett termékeknek.

A biztonsági szakértők az évtized biztonsági eseményének nevezték, a Shell, vagyis bomba elnevezés is a probléma nagyságára utal. A világon az összes felelős nemzeti kibervédelmi intézet – beleértve a magyart is – figyelmeztetést adott ki a sérülékenységgel kapcsolatban, külön oldalt létesítettek a kapcsolatos tennivalók és információk megosztására. Az Amerikai Egyesült Államokban odáig mentek, hogy a per lehetőségét is megemlítették azon vállalatok számára, akik nem frissítik érintett rendszereiket. A támadói csoportok sem tétlenkedtek: a nem túl bonyolult kihasználási lehetőség miatt rögtön felvették eszköztárukba a Log4Shell-t is, mind a szervezetten dolgozó csoportok, mind az állami támogatás élvező hackerek.

Az ellátási lánc biztonságát rendíti meg

Az ellátási lánc biztonságának kérdésével korábban is foglalkoztunk már az IT-BUSINESS hasábjain, de most újból el kell mondanunk, hogy az egymásra utaltság a szoftverfejlesztésben is komoly problémát okoz. A nyílt forráskódú megoldások alkalmazása felgyorsítja a vállalati innovációt, a bizalom megrendülése viszont a fejlődés gátja lehet, hiszen megdrágítja az amúgy sem olcsó szoftverfejlesztést.

A fél világ 2021 decemberében és még most is az érintett rendszerek frissítésével volt elfoglalva. Az első, hibásan frissített Log4j-verzió után gyorsan érkezett egy második patch is, ezt pedig mind be kellett forgatni az érintett megoldásokba. A be nem tervezett patchelés, az esetleges leállás meg újabb költséget generált.

„Az open source világban sajnos előfordulhatnak rejtett »aknák«, amelyek évek múlva a mostanihoz hasonló problémát okoznak", mondja *Tóth Attila,* a német autóipari cégeknek fejlesztő Minero IT (a Gloster egyik. leányvállalata) projektmenedzsere. A nyílt forráskódú világ a fejlesztők együttműködésén és bizalmán alapszik. Mindenki hozzátehet, -fejleszthet egy adott termékhez. A fejlesztéseket természetesen átnézik, ellenőrzik szakemberek. Ha a rejtett sérülékenység átmegy az ellenőrzésen, akkor onnan nincs megállás, sok esetben automatikusan egy szoftver adja hozzá a kiegészítőt a fejlesztéshez.

A projektmenedzser szerint hosszú távon ez az incidens, ahogy a további sérülékenységek is, az open source-on alapuló fejlesztések végét jelenthetik. A világ digitális átalakulását a nyílt forráskódú termékek nagy mértékben felgyorsították, az innovációt egyszerűsítették. A komoly, nagyvállalati fejlesztésekhez hosszú távon nem fogják az open source jelentette kockázatot beengedni. Nem egyik napról a másikra mondanak le a kritikus fejlesztések az nyílt forráskódról, hanem lépésenként: a mellőzés, az ajánlott mellőzés után következhet az egyértelmű tiltás.

A megrendült bizalom miatt a vállalatok inkább kifizetnek egy fejlesztőt, hogy olyan saját kódot írjon, amely bevizsgált, ellenőrzött, és amelyért vállalja a felelősséget. Ha maradnak is az open source megoldásnál, akkor lassabban lehet vele haladni. A koc-

TÓTH ATTILA, MINERO IT

FORRÁS: TÓTH ATTILA

FORRÁS: 123RF.COM

kázatok kiszűréséhez a kódot átvizsgálja az IT-biztonsági csapat vagy a külső szakértő cég. Az is elképzelhető, hogy csak adott szervezetek által bevizsgált és minősített szoftverösszetevőket lehet majd használni. „Ez mind-mind plusz szakértelmet, munkát, azaz plusz költséget jelent szoftverfejlesztés terén”, szögezte le Tóth Attila.

Másképp működik a nyílt és a zárt forrású modell

„A sérülékenység sok munkát adott a szoftverfejlesztőknek és IT-üzemeltetőknek egyaránt, de nem rendült meg a bizalom az open source szoftverekkel szemben”, mondja *Pásztor Tamás,* aki nagy teherbírású IT-rendszerek üzemeltetésével foglalkozik a távközlés és a kereskedelem területén. A nyílt forráskódú rendszerek elterjedtek, rendkívül sok helyen használják őket, mélyen beépültek a szervezetek, vállalatok mindennapjaiba.
A Log4Shell-sérülékenység óriási ijedtséget okozott, mert a rengeteg használatban levő, Java alapú szoftvert gyorsan kellett át vizsgálni, hogy érintettek-e, majd a fejlesztőknek be kellett ütemezni a normális napi működésbe a frissítést. Az érintett, nagy teherbírású és forgalmú vállalati rendszerek esetében maga a frissítés ütemezése sem volt triviális. A frissített komponens beépítése után a fejlesztőknek még tesztelniük is kellett a kapcsolódási pontokat, a szoftver működését, így 1-2 hét is eltelt mire a patchelés végigfutott.

Azonnal felvették eszköztárukba a rendkívül egyszerűen kihasználható Log4Shell-sérülékenységet a támadói csoportok

Az üzemeltetési szakember szerint ez a sérülékenység szemléletváltásra kényszeríti a fejlesztőket és az üzemeltetőket egyaránt, ezentúl a gyorsan változó szoftverkomponensek patchelésére is jobban figyelnek majd. „Főként az alapkomponensek esetében hajlamosak vagyunk megfeledkezni a frissítésről: beépítettük

PÁSZTOR TAMÁS
IT-BIZTONSÁGI SZAKÉRTŐ

FORRÁS: ITB

a szoftverbe, rendeltetésszerűen ellátják munkájukat, nincs más teendőnk. Emiatt rengeteg, régóta kijavítható sérülékenységgel teli megoldás kapcsolódik a publikus internethez, ez pedig komoly biztonsági kitettséget jelent. A támogatási szerződések lejárta után a vállalatoknak legalább a biztonsági frissítésre kellene pénzt és energiát fordítaniuk", fejezte be Pásztor Tamás.

Patchelés vállalati környezetben

A sérülékenység egy másik problémára is felhívta a figyelmet: vállalati környezetben problémát jelenthet a rendszerek állandó frissítése. A rendszerek fontosságától függően a frissítés több hetet is elvehet az IT-csapat munkájából. A patcheket tesztelni kell, mielőtt a kritikus rendszereket frissítik. Az is késleltetheti a frissítést, hogy azt a vállalat különböző okokból ezt nem tartja fontosnak: kicsi az IT-csapat, nincs szakértelem a szervezeten belül, vagy más, fontosabb feladatokra kell a szűkös erőforrás.

A helyzetet az sem segíti, hogy egyre gyakrabban jönnek ki frissítések. Így amikor a rendszergazdák épp végeznek az utolsó simításokkal, máris érkezik az újabb frissítés. Ez önmagában komoly kihívás, de ne feledjük, hogy nemcsak egy szoftver működteti a vállalatot. A Microsoft igyekszik havi egyre csökkenteni a patchek gyakoriságát. A Patch Tuesday-en, vagyis minden hónap második keddjén érkeznek. Az Apple-nél viszont *Tim Cook* vezetése alatt 51 százalékkal nőtt a frissítések gyakorisága.

Kockázat szerinti foltozás

„Hiába töltötte szabadságát jó néhány kolléga december 10–20. között, a Spar Magyarország több mint 150 rendszerét kellett átvizsgálniuk, hogy érintett-e a Log4Shell sérülékenységben", mondta el *Tátrai László,* az üzletlánc IT-vezetője. Az esetleges patch-elést megnehezítette, hogy az első körben kiadott javítás egy másik sérülékenységet tartalmazott, tehát a már kijavított rendszerekkel újból kellett foglalkozni. Volt olyan rendszer, ahol a gyártó nem tudott időben információt adni az érintettséggel kapcsolatban, ezért ezeket ideiglenesen lekapcsolták. A teljes hálózati infrastruktúrát megerősítették, hogy az esetlegesen érintett rendszereket minél előbb izolálni lehessen. A sérülékenység szerencsére nem érintette a saját fejlesztésű árugazdálkodási rendszert, az élelmiszer-termelési üzemekben használt megoldásokat és a kasszarendszereket sem.

Nemzetközi szinten 2021 elején kezdtek el a cégnél kiemelten és komolyabban foglalkozni az IT-biztonsággal. Az ösztönözte őket leginkább, hogy sajnos két osztrák cég is zsarolóvírusos támadást szenvedett el. Az IT-vezető tájékoztatása szerint cégüknél a nemzetközi Data Security csoport mellett Ausztriában felállítottak egy Security Operation Centert (SOC-ot), amely az összes leányvállalat IT-biztonságával foglalkozik. Innen folyamatosan monitorozzák a hálózati forgalmat, állandó a sérülékenységvizsgálat is, automatizmusok vagy szakemberek segítségével az összes anomáliával foglalkoznak.

A cégnél biztonsági szempontból elemezték és rangsorolták az összes üzleti IT-rendszert, így állapították meg, hogy mely rendszerrel milyen szinten kell foglalkozniuk. A jellemzően Windows alapú kliens környezet patchelése a kockázatok és előre meghatározott menetrend szerint történik – hacsak nincs a Log4Shellhez hasonló kritikus sérülékenység.

A Tier3 kiszolgáló rendszereiket automatikusan frissítik, a Tier2 és Tier1-es rendszereket pedig csak tesztelés és minőségbiztosítás után. A Tier1 rendszerek esetében csak akkor van patchelés, ha van működő, kipróbált, rollback- (visszaállító) folyamat a háttérben. Vannak régi rendszerek, amelyeket nem tudnak frissíteni, ott hálózati izolációval védekeznek, csak a minimálisan szükséges forgalmat engedélyezik.

Az alapfelfogás a vállalatnál, hogy a telepített rendszereken a hálózati forgalom alapból tiltott. A felhasználók és az üzlet igénye szerint folyamatosan engedélyezik a szükséges forgalmakat.

A fizikai biztonságra is figyelnek, kártevőt tartalmazó USB memóriákkal náluk hiába próbálkoznak. „Néha paranoiásnak tartanak vállalaton belül, de az erős IT-biztonságot csak fokozottan ellenőrzött és kontrollált körülmények között tudjuk megteremteni", hangsúlyozza Tátrai László.

A tanulság, hogy a biztonsággal mindenképp érdemes foglalkozni, lehetőség szerint már a tervezés fázisában. Hogy a sorozatos biztonsági incidensek végül a nyílt forrású fejlesztések végét hozzák, vagy a gyorsabb fejlesztés miatt a cégek inkább bevállalják a magasabb biztonsági kockázatot? Ki fog derülni.

Vass Enikő

TÁTRAI LÁSZLÓ, SPAR MAGYARORSZÁG

FORRÁS: SPAR MAGYARORSZÁG

Népszerűtlen a cégeknél a frissítés

Az Ivanti 500 IT-szakember megkérdezésével készített felmérése szerint a CIO-k 71 százaléka túl bonyolultnak, nehézkesnek és komplexnek tartja az alkalmazások és rendszerek frissítését. Az is problémát jelent számukra, hogy a feladat túl sok időt vesz el az értékesebb munkától. Erre a cégvezetők hozzáállása is rátesz egy lapáttal: az IT-szakemberek közel kétharmada (61 százaléka) szerint a cégvezetők negyedévente egyszer kérik a frissítések elhalasztását, mondván, az üzletkritikus rendszerek nem állhatnak le. Ezzel pedig komoly biztonsági kockázatokat vállalnak fel.