KÉTLÉPCSŐS AZONOSÍTÁS

Apró lépés a százszázalékos biztonság felé

FORRÁS: STEVANOVICIGOR / VALERY BROZHINSKY / GETTY IMAGES

Használjunk kétfaktoros azonosítást a vállalati rendszerekbe történő belépéskor, kis befektetéssel óriásit lendítünk cégünk biztonságán. Második azonosítóként ne a kényelmes, hanem a biztonságos lehetőséget használjuk, legyen az hardveres vagy szoftveres token, push-üzenet vagy biometria.

Egy kicsi, ámde annál fontosabb változást jelentett be július elején a Google: azoknál a felhasználóknál, akik két faktoros azonosítást állítottak be, a második azonosítót immár nem SMS-ben, hanem push-üzenetben küldi ki.
A sok millió felhasználót érintő változás azért érdekes, mert az SMS biztonsági problémáira rég felhívták a szakértők a felhasználók figyelmét, ámde sokan még mindig az SMS-t kedvelik második azonosítási faktornak.
Ezzel nem azt mondjuk, hogy most rögtön mindenki menjen cserélje le az SMS-t egy más faktorra. Ha egy vállalat, szolgáltató egyáltalán két faktort használ felhasználói azonosítására, azzal már rengeteget tesz annak érdekében, hogy növelje a vállalat biztonsági szintjét. Azonban, ahogy a LastPass felméréséből kiderül, a vállalatoknak csupán 57 százaléka használ multifaktoros azonosítást (igaz, ez 12 százalékpontos emelkedést jelent a korábbi felmérésükhöz képest).

Jelszóval próbálkoznak a támadók

Pedig a vállalatoknak elemi érdeke lenne a második autentikációs faktor bevezetése, hiszen segítségével a külső támadásokat sikeresen hárítanák. A Verizon Data Breach Investigations Report 2020 kutatása szerint a támadók inkább lopott vagy elhagyott azonosítókat használnak, mintsem kártevővel fertőzzék meg a kiszemelt szervezetet. Az első számú támadás 45 százalékkal a hackelés maradt, mely a jelszavak megfejtését gépi segítséggel, az elveszett vagy ellopott jelszavak használatát is magába foglalja. Tehát a vállalatok saját jól felfogott érdeke, hogy ezeket a támadásokat egy második azonosító használatával is igyekezzenek megfogni. Hiszen a támadók is emberből vannak, és legtöbben feladják a, ha látják, hogy a jelszó után még egy második azonosítási faktor megfejtésével is foglalkozniuk kellene. Túl nagy erőfeszítést igényelnek a kétfaktoros azonosítóval védett rendszerek, a könnyebb ellenállás felé fordulnak a támadók is.

Szabályozó is kötelezhet rá

Ahol a józan ész nem kerekedik felül, ott a szabályozó teszi kötelezővé a második azonosítási faktort: az EU-s pénzforgalmi irányelv (PSD2) értelmében például a pénzügyi szolgáltatók számára tette kötelezővé a kétfaktoros azonosítást. A netbankba már csak kétfaktoros azonosítás után lehet belépni, ahogy minden ötödik érintés nélküli vásárláskor meg kell adjuk PIN kódunkat. A bankkártyás online fizetésnél viszont 2020 szeptemberére halasztották az erős ügyfél-hitelesítés bevezetését.

Nemcsak az ujjlenyomatot lehet biometrikus azonosítóként használni

Az arcfelismerést az Apple tette népszerűvé, de már a legtöbb androidos telefonban is benne van. A technológia most nem várt helyről kapott pofont: a maszkot hordó embereknél használhatatlan. Pedig Már előtte is gondja akadt a nem fehér emberek felismerésével, az ázsiai vagy afrikai eredetű felhasználók esetében tízes nagyságrenddel több esetben oldotta fel a készüléket más felhasználók arcára is, gyakori a hamis pozitív eredmény.
Az infravörös vénaszkenner az arcfelismerésnél kiforrottabb technológia, mely a tenyérvénák mintázata alapján azonosítja az embereket. (Az oxigénszegény vért szállító vénák sötétebbek, mint az artériák.) A vénaszkenner hőtérképet is készít, így viasztenyérrel, tenyérfotóval, cadaverrel nem csapható be. A mögöttes technológia ára és a leolvasó mérete jelenti a használati korlátokat. *(A budapesti Groupama Arénában helyeztek üzembe Fujitsu vénaszkennert.)*
A viselkedésminta alapú azonosításban is látnak fantáziát a szakemberek. Nem egyszeri, hanem folyamatos ellenőrzést biztosíthat a munka során. Irodai környezetben ez abban merülne ki, hogy miután egy adott felhasználót azonosítottunk, figyelhető, hogyan mozgatja az egeret, milyen sebességgel gépel, milyen tipikus hibákat vét, ahogy azt is követheti, milyen alkalmazásokat használ és milyen adatokhoz fér hozzá. Pár órás megfigyelés alatt nagy megbízhatóságú profil alakul ki. Ha a rendszer eltérést tapasztal, a felhasználó kockázati szintjét megemeli, majd a beállított riasztási szint felett le is tilthatja a további tevékenységektől.

Nem szeretik a biometrikus azonosítót

Nem egyszerű feladat kiválasztani, hogy mi legyen a második azonosító, választhatunk a szoftveres token, hardveres token, SMS, biometrikus azonosító, push-üzenet között, illetve a lapzártakor megjelent BM rendelet szerint akár e-személyit is.
Ha a felhasználókra bízzuk a választást, és a népszerűség szerint választanánk második autentikációs faktort, akkor az a hardveres token lenne. Vállalati környezetben vannak olyan szervezetek, amelyek vállalják ennek az autentikációs formának a költségeit, viszont a fogyasztókkal való kapcsolattartásban a második helyezett SMS divatos. (A Specops vállalat kutatását vettük alapul.)
A kutatásnak az az érdekessége, hogy a lista második felében, vagyis a kevésbé kedvelt autentikációs módszerek között (50 százaléknál kevesebben választották) a biometrikus azonosítók voltak, legyen az az ujjnyomat, arcfelismerés, írisz felismerés, retina szkennelés. A biometrikus azonosítók használatától azért

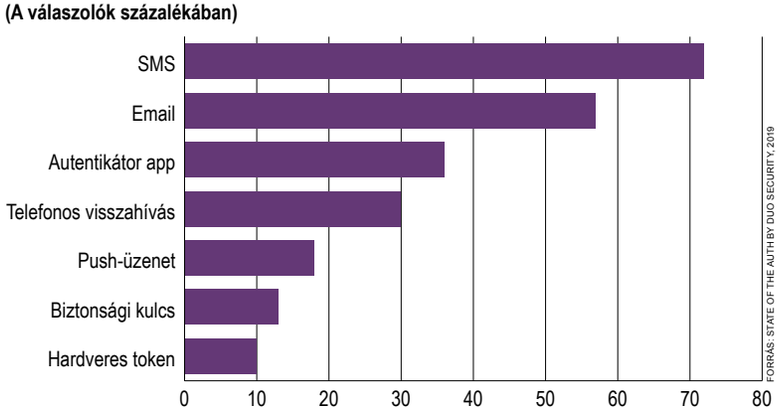
FORRÁS: CSOONLINE.COM

tartanak az emberek, mert azokat nem módosíthatjuk. Ha a nem megfelelően tárolt biometrikus azonosítók kiszivárognak, akkor teljes egészében le kell mondjunk használatukról. Pedig kényelem szempontjából ez a legjobb választás: mindig velünk van, sohasem felejtjük el.

Az SMS a leggyakoribb második faktor

A Duo Security 2019 decemberében kiadott, kétévente megismételt kutatása szerint a második autentikációs faktor közül az SMS üzenet a leggyakrabban használt, az esetek 72 százalékában fordulnak ehhez, második az email 57 százalékkal, harmadik az autentikátor alkalmazás 36 százalékkal (több opciót választhattak a válaszadók). Az SMS népszerűsége azzal magyarázható, hogy nincs szükség külön alkalmazás telepítésére a felhasználó eszközén, a régebbi készülékeken is működik.
Az SMS népszerűsége annak ellenére komolyan tartja magát, hogy nem is a legygyorsabb. A push-üzenetek például gyorsabban érkeznek, éves szinten 13 percet spórolnak meg egy átlag felhasználónak. De ha ez a közel negyedórányi veszteség nem is számítana, a biztonsági problémák gondolkodóba ejthetnének.

2FA autentikációs megoldások használatuk szerint
(A válaszolók százalékában)



FORRÁS: STATE OF THE AUTH BY DUO SECURITY, 2019

Sajnos, az SMS nem biztonságos

Az SS7 (Signaling System #7) telefonos protokoll miatt vannak veszélyben az SMS üzenetek. Az 1975-ben kifejlesztett protokoll szabályozza a hívás továbbítást, a számlázást, a szöveges üzenetek küldését. Segítségével állapítják meg, hogy egy SIM-kártya még mindig használatban van vagy sem. Lehetővé teszi a számok hordozását, hogy a szolgáltatók egy mobiltelefon földrajzi helyzetét bemérjék 50 méteres pontossággal.
Erre nem azért van szükség, mert kémkedni szeretnének utánunk, hanem azért, hogy a szolgáltató az egyik adótoronyból a másiknak adja át a hívást. E nélkül például az autós mobilhívás megszakadna, miután az eredeti kapcsolatot létrehozó adótorony hatósugarából kikerülünk.
Az SS7 protokoll kihasználása inkább elméleti lehetőség, mintsem elterjedt módszer a második azonosító megszerzésére. Viszont a, „SIM swap” vagyis a SIM kártya kicserélésének módszere sokkal elterjedtebb, inkább az Amerikai Egyesült Államokban és Nagy-Britanniában, de sajnos, már itthon is volt rá példa.
A lényeg, hogy a bűnözők megszerzik a mobilszámot, adatainkat, majd a mobilszolgáltatónál kérnek egy másik mobilszámot, a régire érkező üzeneteket, hívásokat pedig átirányítják az új számra. Ebben az esetben is meg kell szerezni a felhasználó adatait, banki azonosítóit, és csak azután érkezhet a kicserélt telefonszámra a második autentikációs faktor.
Ami maradt a második azonosítók közül – a szoftveres vagy hardveres token és a saját alkalmazásból vagy szerverről küldött üzenet, vagyis a push-üzenet, esetleg telefonos visszahívás – mind biztonságos, ámde nem nagyon kényelmes megoldás. Ne ijedjünk meg használatuktól, hiszen a kollégák, az ügyfelek is belátják, hogy a biztonsági szint növelése csak így érhető el.

Vass Enikő

Az ICT-piac Nagykönyve 2020

Megjelenés: 2020.09.01.

ITB innovációs díj
ITBUSINESS AWARD – Bemutatjuk a Termékfejlesztés és a Projektbevezetés kategória pályázóit.

Almanach
Cégbemutatók és interjúk

Melyek azok az ICT-technológiák, amelyekre B2B-szempontból vevők az ügyfelek 2020-ban és 2021-ben?

Automatizáció, robotika, drónok
Két szempontból is előtérbe kerültek ezek a technológiák az elmúlt hónapokban, egyrészt a járványhoz hasonló helyzetben kieső emberi munkaerő pótlása miatt, másrészt a gazdasági válságban a hatékonyság fokozása érdekében érdemes bevetni ezeket. Az ITBUSINESS összeállításában bemutatjuk, mekkora piaci potenciált látnak az elemzők ezekben a technológiákban, mennyire gyorsulhat fel a fejlesztésük, tényleg átveszik-e az emberek helyét a robotok.

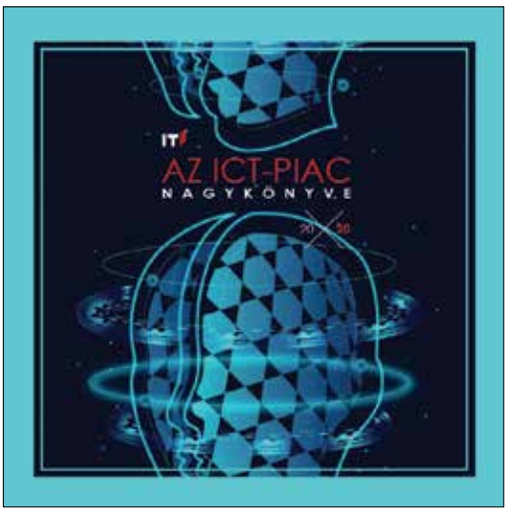
Csoport- és távoli munkát támogató megoldások, kommunikációs platformok és szoftverek Forradalmi változásokat indított a kapcsolattartásban és a csoportmunkában a koronavírus-járvány, kiderült, hogy több kontinensről, akár több tucat ember egyszerre tud hatékonyan és eredményesen résztvenni stratégiai fontosságú megbeszéléseken is, üzleteket lehet összehozni a virtuális térben, többkörös tendereket lebonyolítani. Az elmúlt hónapokban gyűjtött tapasztalatok alapján szinte biztos, hogy a jövőben is fokozottan használják majd céges környezetben is ezeket a technológiákat. Abban is biztosak lehetünk, hogy a gyártók további fejlesztésekkel, kényelmi funkciókkal és izgalmas dizájnnal dobják majd fel megoldásaikat, az ITBUSINESS pedig a kínálkozó üzleti lehetőségekről, a fejlesztési irányokról is beszámol összeállításában.

5G
Hivatalosan is megérkezett Magyarországra az 5G, már két szolgáltatónál is elérhető kereskedelmi megoldásként, a nagy kérdés, hogy mire fogjuk használni. A szakértők szerint az igazán nagy robbanást az üzleti alkalmazása jelenti majd, de mit takar ez, milyen területeken alakíthatja át teljesen az életünket, hogyan hat a gyógyításra, elhozza-e a közlekedés forradalmát, még jobban felpörgeti-e a most zajló ipari forradalmat - ezekre a kérdésekre keressük a választ az ITBUSINESS összeállításában.

Netezünk a televízión, a hűtőnk akár magától tudna rendelni ételt, a sütő pedig izgalmas receptekkel bombázhatja gazdáját
Az internethez kapcsolódó eszközök elárasztották a háztartásokat. De egyre több okosmérő jelenik meg a világban, szenzorok kerülnek szinte mindenhova és egyre elképesztőbb becslések látnak napvilágot arról, hogy hány milliárd eszköz kapcsolódik majd a világhálóra pár éven belül. Az IoT, vagyis a dolgok internete nem új dolog, de az új technológiák és érzékelők egészen izgalmas felhasználási területeket nyitnak, az ITBUSINESS pedig bemutatja az új üzleti lehetőségeket.

Biztonság, GDPR, adatvédelem, adatkezelés
A távmunka, online rendezvények és általában a járványhelyzet rávilágított, hogy a biztonságra és adatvédelemre, az adatok kezelésére jobban oda kell figyelni, hiszen IT-biztonsági megoldásokkal kevésbé körülbástyázott környezetekben folyik a munka. Összeállításunkban megnézzük, milyen kihívások elé állították az IT-biztonság, GDPR, adatvédelem és adatkezelés kérdését a digitalizálódó világ, milyen trendekre kell felkészülni ezeken a területeken.

Felhő
A felhőtechnológia minden vállalat életében jelen van, még ha erről nem is tudnak. Összeállításunkban megnézzük, milyen



trendek érvényesek a felhőtechnológia területén, hogyan jelennek meg ezek a vállalatok mindennapjaiban, és milyen speciális gondokkal, kihívásokkal küzdenek a magyar vállalatok ezen a téren.

Pénzügyi digitalizáció
A fintech szektor aranykora az érintésmentes világ megerősödésével jött el, amikor a kormányzati szereplőktől kezdve még a sarki zöldséges is felismerte, hogy a digitalizáció ezen a téren elkerülhetetlen. A pénzügyi digitalizáció trendjeit, a készpénzmentes világ felé vezető út akadályait igyekszünk összeállításunkban felvillantani

Egészségügyi informatika
A járványhelyzet ismételten megmutatta, hogy a fejlett egészségügyi rendszerek szó szerint élet-halál kérdését jelentik. A cikkben megnézzük, hol tart az e-egészségügy a világban és Magyarországon, annak különféle aspektusaival, a közegészségügyi rendszerektől az MI-t alkalmazó diagnosztikai rendszereken át a pácienseket segítő mobil appokig és okos eszközökig.

Mesterséges intelligencia
Az MI hatásairól, gazdaságélénkítő potenciáljáról sokat hallhattunk, a gyakorlati, használható megvalósítások viszont ritkábban kerültek előtérbe. Néhány működő példán keresztül mutatjuk be, mire is képes az MI.

Folyamatok menedzsmentje és automatizációja
Amikor egy vállalat kénytelen távmunkában dolgozni, felértékelődnek a jól szabályozott céges folyamatok, amelyek végrehajtása nem függ attól, hogy a kollégák egy szobában ülnek-e vagy sem. A hatékony folyamatmenedzsment nem csak a munkavégzést függetleníti annak fizikai helyszínétől, de az ellenőrzést is megkönnyíti. Egyúttal arra is rámutat, hogy mennyi manuális munka lenne kiváltható folyamatautomatizációval (RPA-val).

Kormányzati informatika
Szakmapolitikusokat, állami vállalatok vezetőit kérdezzük, hogy élték meg az elmúlt egy évet? Mik az elmúlt 12 hónap mérföldkövei? A COVID-19, az újraindítás mennyiben nyomta rá bélyegét tevékenységükre?
Sorra vesszük, milyen személyi változások történtek tavaly szeptembertől.

TOP 25
Debütál az elmúlt 12 hónap 25 legsikeresebb hazai ICT-menedzsereinek toplistája!