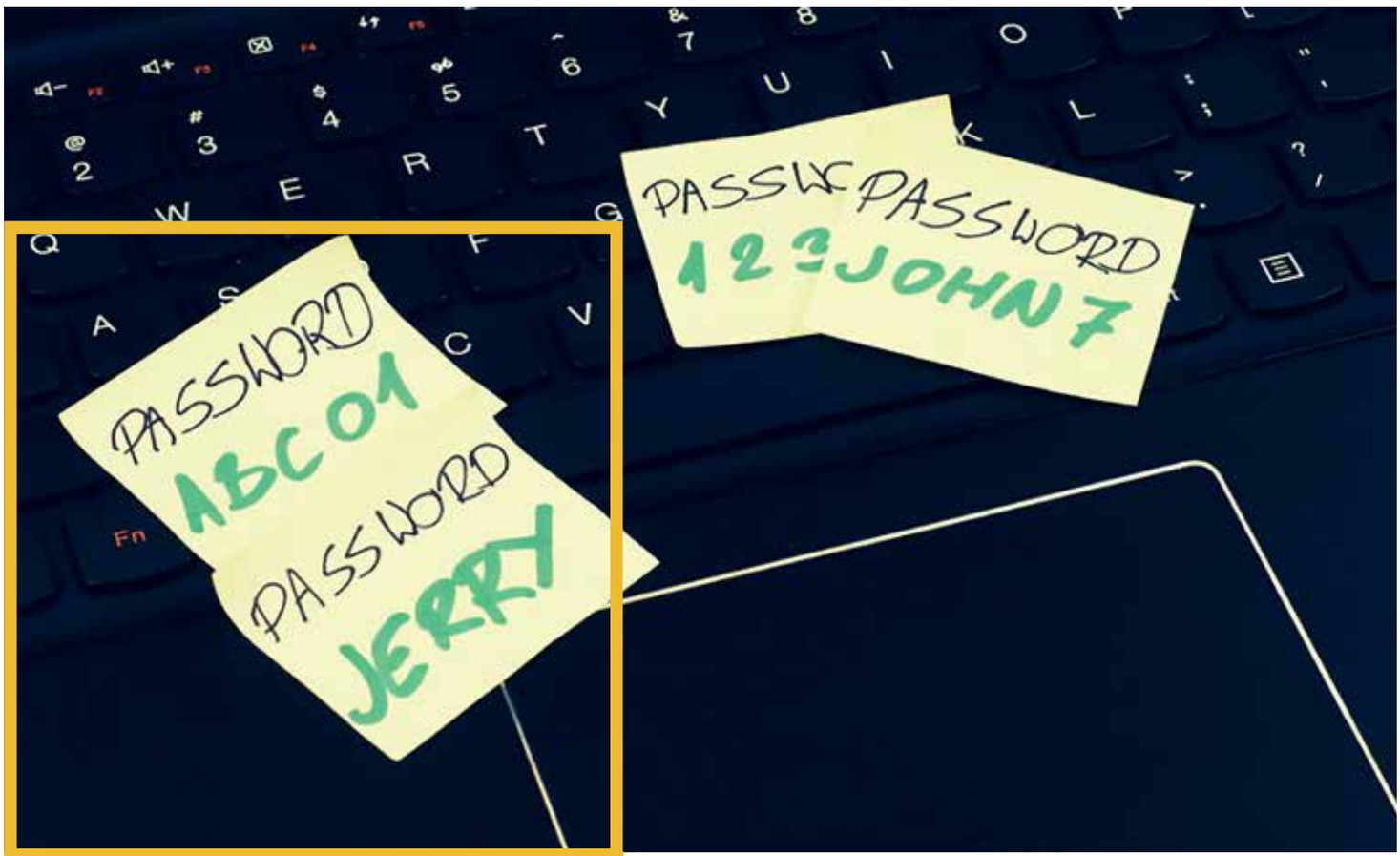


FORRÁS: BLOG.MALWAREBYTES.COM

ROSSZ A VÁLLALATI JELSZÓHIGIÉNIA

Elvesznek a kollégák a jelszavak dzsungelében

Vállalati szinten átlagosan 55 jelszót kellene észben tartania egy alkalmazottnak, ami, lássuk be, lehetetlenség. Ez a rengeteg jelszó oda vezet, hogy a vállalati „higiénia" kívánnivalót hagy maga után. Segíthetne a biztonságosságon, ha a cégek eltörölnék a havonként kötelező jelszócserét és – ahogy az sok vállalatnál már gyakorlat – bevezetnék a kétfaktoros azonosítást.

Szükséges rossz, hogy az online világban az azonosításhoz jelszavakra van szükségünk. Az alkalmazottak nem szeretik, mert egy újabb nyűg, amit észben kell tartani, a rendszergazdák is utálják, mert folyamatosan ki kell kényszeríteniük valahogy az emberekből a minőségi jelszavak használatát, és ráadásul sok helyen minden hónapban újra kezdődik ez a tortúra.

Rengeteg jelszót kell megjegyezni

A felhő alkalmazások és a mobilappok terjedése, az egyéb rengeteg új technológiai eszköz mind újabb és újabb jelszót jelent. És az emberek végleges kapacitással rendelkeznek, amikor jelszavak megjegyzéséről van szó, ami rendkívül rossz jelszó higiénia kialakulásához vezet: a jelszavakat újrahasznosítják, leírják papírra stb. A kisebb vállalatoknál egy alkalmazottnak átlagosan 85 jelszót kellene észbe tartania, míg a nagyobb vállalatoknál csupán 25 jelszóról beszélünk, vagyis átlagosa 55-öt – derül ki a LastPass kutatásainak adataiból. A nagyobb vállalatoknál jobban elterjedtek a Single Sign On- (SSO-) megoldások, amikor egyetlen vállalati belépéssel rengeteg megoldáshoz, erőforráshoz juthatnak hozzá a kollégák. A nagyobb cégeknél ugyanakkor elterjedtebbek az IT-biztonsági előírások is, melyek meghatározzák (jellemzően letiltják), hogy milyen külső szolgáltatásokat lehet igénybe venni. Összességében a vállalatok kevesebb mint felénél van SSO-megoldás.

Az FBI és a szakértők is a 16 karakternél hosszabb, de könnyen észben tartható jelmondatok használatát javasolják a speciális karaktereket, nagybetűt és számot is tartalmazó, komplex jelszó helyett

Újrahasznosított jelszavak

A jelszó-újrahasznosítás is valós jelenség, a felmérés szerint egy tipikus alkalmazott átlagosan 13 különböző alkalmazásban használja újra ugyanazt a jelszót. A mikrovállalatoknál (az 1-25 fős cégeknél) a legrosszabb a helyzet, ugyanis a maximum 25 alkalmazottal rendelkező cég esetében 14 alkalommal hasznosítják újra a jelszót, míg a több mint tízezer fős vállalatoknál ez a szám négy. A média-, illetve reklámiparban a legrosszabb a helyzet, ott átlag 23 különböző alkalmazásnál használják ugyanazt a jelszót. Ezt a szektort követi a technológia- és a szoftver-iparág és a távközlés 15-13 újrahasznosított belépési azonosítóval. A legjobb a helyzet a kereskedelemben és a nonprofit szervezeteknél, csupán 9 újra hasznosítással.

A média- és reklámiparban dolgozók egyedüli mentsége a magas arányú jelszó-újrahasznosításra az, hogy ők eleve rengeteg, jelszóval védett alkalmazást, webes szolgáltatás kénytelenek használni: egy alkalmazottnak 97 jelszót kellene megjegyeznie, míg a skála másik végén lévő kormányzati szektorban csupán 54-et.

A jelszavak megosztása is megszokott és rossz gyakorlat a vállalatoknál. Nagyon sok részlegnél vagy csoportnál csak egy-két szoftverlicencet vásárolnak, holott ennél többen használják az adott alkalmazást – a felhasználók között külső partnerek is előfordulhatnak.

Valójában nem kell a kötelező csere

A rengeteg jelszó megjegyzését váltaná ki többek között, ha a rendszergazdák kivezetnék az általános gyakorlatból a jelszavak időnkénti kötelező cseréjét. Ez a gyakorlat azután terjedt el, hogy az Amerikai Szabványügyi Hivatalnál dolgozó *Bill Burr* 2003-ban ezt a javaslatot megfogalmazta, a fejlesztők pedig beépítették alkalmazásaikba. Maga, az azóta visszavonult szakember és a biztonsági szakértők egyöntetű véleménye szerint a vállalatok és az alkalmazottak életét megkönnyítené, és biztonság szintjét is emelné, ha csak akkor változtatnánk jelszót, ha felmerült annak gyanúja vagy biztosak vagyunk benne, hogy az kiszivárgott.

A multifaktoros azonosítás áll nyerésre

Egyre több vállalatnál használják a multifaktoros azonosítást, a kutatás szerint 12 százalékponttal, 57 százalékra növekedett a több azonosítási módszert kombináló vállalatok száma. Ez azt jelenti, hogy a vállalatok komolyan veszik a jelszavak biztonságát a belső vállalati környezetben is.

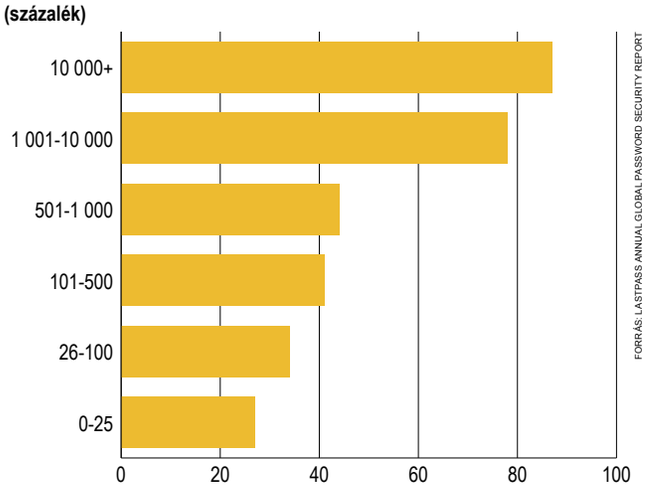
A jelszó mellett a szoftver alapú azonosítási faktor az egyértelmű nyertes a vállalatoknál, a multifaktoros azonosítást használó alkalmazottak 95 százaléka ugyanis szoftveres alapú azonosítást használ második opcióként, például egy mobilappot (legyen az a LastPass Autheticator, Duo Security, Google Authenticator, hogy a három legnépszerűbbet említsük). A vállalatoknak csupán 4 százaléka használ hardver alapú, és 1 százaléka biometrikus azonosítást. A szoftveres megoldás népszerűségét annak méretezhetősége, gyors bevezethetősége és alacsony költsége magyarázza.

Az sem meglepő, hogy egyes iparágak proaktívabban használják a kétfaktoros azonosítást, mint mások: a technológia-, illetve a szoftverszektorban tevékenykedő vállalatoknál használják a legmagasabb arányban, míg a nonprofit szféra, média- és reklámcégek, illetve a jogi és biztosítói szektor a végén kullog a biztonságosabb belépés elfogadásában.

A vállalat méretét tekintve minél nagyobb egy vállalat annál, nagyobb a gyakorisága, hogy az alkalmazottak használnak kétfaktoros azonosítást: a nagy vállalatok 87 százalékánál elterjedt, míg a mikrovállalatoknál csupán valamivel több mint negyedük használja. Ez felelőtlenség a kisebb vállalatok részéről, hiszen a támadások közel fele őket veszi célba, az egyfaktoros azonosítás pedig a kiberbűnözők tevékenységét segíti. Az a tény sem segít, hogy a Verizon kutatása szerint a kkv-k 60 százaléka fél éven belül bezárja a kapuját egy sikeres kibertámadás után.

Vass Enikő

A kétfaktoros azonosítást használó vállalatok aránya vállalatméret szerint



A felmérésről

A LastPass Annual Global Password Security Report jelentésében több mint 47 ezer vállalati ügyfelétől származó, anonimizált felhasználói adatok elemzett. Noha a vállalatok mind a LastPass ügyfelei, a minta sokasága miatt a jelentésben foglaltak a vállalatok többségére általánosan érvényes következtetéseket tartalmaz.