Egyetemi hálózat biztonságának javítása könnyen használható kétfaktoros azonosítás használatával

Dr Takács Anna Mária, Nemes Teréz, Dr Szobonya Réka

Budapesti Gazdasági Egyetem, Pénzügy és Számviteli Kar, Alkalmazott Kvantitatív Módszertan Tanszék

Budapest, Buzogány u. 10-12, 1149

takacs.anna@uni-bge.hu, nemes.terez@uni-bge.hu, szobonya.reka@uni-bge.hu

Abstract: Security of the networks we use has become a key concern over the years. Both operators and users should be aware of countless different attack methods and defense strategies. In education, including higher education, we want to believe that the risk is lower than in the case of business and other profit-oriented systems. Since the Kréta system and Neptun are based on a common code base, the hacking of Kréta and the leaking of part of the source code may have indicated that the systems used by universities will also become targets. It received less publicity, but it is known that several Hungarian higher education institutions had to deal with various degrees of security damage to their Neptun system. Other systems used in education are also under increasing pressure. In most of the higher education institutions, lecturers are authenticated using a pair of username and password, the disadvantages of which have long been known. Some universities have made the use of their network more secure by implementing two-factor authentication, primarily based on smartphone authenticators or OTP identifiers received by email. However, the use of these solutions often involves more inconvenience for users in addition to increasing security. In this article, we would like to show a method for the possibility of two-factor authentication in university systems, which is basically like a one-factor authentication for instructors. Its use is therefore convenient, so it can be more widely accepted and can provide adequate security for authentication.

Keywords: network security, two-factor authentication, biometric authentication, Yubikey

Összefoglalás: Az általunk használt hálózatok biztonsága kulcsfontosságú kérdéssé vált az évek során. Megszámlálhatatlan különböző támadási módszernek és védekezési stratégiának kellene tudatában lennie az üzemeltetőknek és a felhasználóknak is. Az oktatásban, ebbe beleértve a felsőoktatást is, szeretnénk elhitetni magunkkal, hogy kisebb a veszély, mint az üzleti élet és egyéb profitorientált rendszerek használata esetén. A Kréta rendszer feltörése és a forráskód egy részének kiszivárgása a közös kódalap miatt jelezhette, hogy az egyetemek által használt rendszerek is célponttá fognak válni. Kevesebb nyilvánosságot kapott, de ismert, hogy több magyarországi felsőoktatási intézménynek is

meg kellett küzdeni a Neptun rendszerének különböző mértékű kompromittálódásával és a többi oktatásban használt rendszer is egyre nagyobb nyomásnak van kitéve. Az oktatók hitelesítése a felsőoktatási intézmények többségében felhasználó név és jelszó használatával történik, amely módszernek a hátrányai régtől ismertek. Néhány egyetem a kétfaktoros azonosítás bevezetésével tette biztonságosabbá a hálózata használatát, elsősorban okostelefonos autentikátorokra vagy emailben érkező OTP azonosítóra alapozva. Ezen megoldások használata azonban gyakran több kényelmetlenséggel is jár a biztonság növelése mellett. Ebben a cikkben mi szeretnénk egy olyan módszert mutatni a kétfaktoros azonosítás lehetőségére az egyetemi rendszereknél, amely alapvetően az oktatók számára olyan, mintha egy egyfaktoros hitelesítés lenne. Használata emiatt kényelmes, így nagyobb elfogadottsága lehet és a hitelesítéshez megfelelő biztonságot tud nyújtani.

Kulcsszavak: hálózatbiztonság, kétfaktoros autentikáció, biometrikus azonosítás, YubiKey

1 Egyetemi rendszerek biztonsági fenyegetettsége

2023. április 23-án 20:00-kor összeomlott az informatikai rendszer a Pécsi Tudomány Egyetemen. Leállt az egyetemi wifi hálózat és a hallgatókat kiszolgáló rendszerek. A hallgatói információs rendszer, a Neptun is leállt. Az egyetem adminisztrációját átmenetileg manuálisan tudták elvégezni. Később a szinkronizálás is újabb hibalehetőségeket rejtett magában. A javítás, a hiba elhárítása több napig tartott. Az anyagi kárt nehéz megbecsülni, de óvatosabb becslések szerint is milliós nagyságrendű lehet. Elég nyilvánvaló jelek valószínűsítették, hogy szándékos hackertámadás áldozata lett a PTE informatikai bázisa. Vírus támadás miatt leállt a Pázmány Péter Katolikus Egyetem Neptun tanulmányi rendszere is. Éppen aznap éjfélig lehetett volna feltölteni a szakdolgozatokat a rendszerbe. Természetesen a beadási határidőt meghosszabbították. Hackertámadás, valamint adathalász e-mailek segítségével támadást kezdeményeznek a Szegedi Tudományegyetem rendszerei ellen. Az egyetem üzemeltetői megfelelő felhasználói tudatosságot kértek, mint a hallgatóktól, mint az oktatóktól. Bár viszonylag kevés a megbízható hír került ki róla, több információ is ismert arról, hogy feltörték több másik hazai egyetem Neptun rendszerét is és jelentek meg ott furcsa, trágár üzenetek. A Budapesti Corvinus Egyetem, az ELTE, az Óbudai Egyetem, a Nemzeti Közszolgálati Egyetem, a BME és a BGE is a megemlített egyetemek között volt. Több helyen a Neptun rendszert egy időszakra le is állították. Több érintett egyetemen arra kérték a hallgatókat és oktatókat, hogy a jelszavaik védelme érdekében azokat senkivel ne osszák meg, változtassák azonnal meg és erős, kellően bonyolult jelszavakat használjanak.

Illúzió lenne azt gondolni, hogy az egyetemek informatikai rendszerei nem lesznek további támadásoknak kitéve. Az általános informatikai és hálózatbiztonsági trendeket megvizsgálva látszik, ahogy az egyes szervezetek napjainkban a mindennapi munkájukat az informatikai rendszereikre alapozzák, így az érzékeny adatok védelme és a zavartalan működés biztosítása kritikus fontosságúvá válik. A támadások és adatvédelmi incidensek rapid módon növekvő számától és a támadási módszerek egyre kifinomultabbá válásától a rendszereket használók kevésbé tudatos informatikai rendszer használata és biztonsági képzettsége rávilágít a robusztus IT és hálózatbiztonsági intézkedések fontosságára. [1]

Néhány statisztikai adatot szeretnénk bemutatni a tézis alátámasztására olyan törési módszerekről, amelyek az egyetemi rendszerek feltörésében is szerepet játszottak. 2022-ben 493,33 millió ransomware támadást észleltek a szervezetek világszerte. Az adathalászat továbbra is a leggyakoribb támadás forma, naponta körülbelül 3,4 milliárd spam e-mail érkezik Az adatszivárgás globális költsége 4,35 millió dollár volt 2022-ben. Az ellopott vagy feltört hitelesítő adatokból eredő jogsértések átlagos költsége 4,50 millió dollár volt. 4,1 millió webhely fertőzött meg rosszindulatú programokkal. A webhelyek 18%-a pedig kritikus kiberbiztonsági fenyegetéseket tartalmaz. [2] Annak bizonyítására, hogy a támadások volumene áthelyeződik a tudományos és oktatási környezetek felé, a LinkedIn az adathalászattal kapcsolatos támadások 52%-ával volt kapcsolatban világszerte. Ez volt az első év, amikor a világ legnagyobb szakmai közösségi oldala szerezte meg ennek a kétes értékű rangsornak az első helyét, jelezve a probléma súlyosságát és a súlypontok áthelyeződését. Az egyik legnagyobb egyetem támadásánál zsarolóvírus-támadási vektor is szerepet játszott. 2022-ban ez a támadási módszer jelentős, 21%-os csökkenést mutatott az előző évhez képest. 493,3 millió ransomware-kísérlet történt, miközben 2020-ban 62%-os, 2021-ben pedig 105%-os emelkedés következett be a zsarolóvírusok használatában. Ez azt mutatja, hogy ennek a támadási módszernek felismerésére és kivédésére a rendszerüzemeltetők már sokkal jobban felkészülhettek.

Az érintett egyetemek rendszereihez a támadó egy-egy hallgató vagy oktató jelszavának megszerzésével fért hozzá és tudott rendszerkritikus és trágár üzeneteket küldeni a hallgatóknak és oktatóknak. Sajnos a magyar felsőoktatás esetében eddig az időpontig a rendszereknél alkalmazott autentikáció a felhasználói név és jelszó páros, például maga a Neptun rendszer kódszinten sem alkalmas sem más módszeren alapuló hitelesítési lehetőségre, sem a biztonságot növelő egyéb módszerek alkalmazására. A username-password páros alapuló hitelesítés nagyon sok alapvető biztonsági problémát vet fel. 2019-ben az összes adatvédelmi incidens 80%-át a feltört jelszavaknak tulajdonították, azóta a helyzet nem igazán javult ebben a szegmensben. A felhasználók jelszóhasználati szokásai nem is igazán engedik meg a javulás lehetőségét. A felhasználók 49%-a csak egy betűt vagy számjegyet változtat meg a preferált jelszavában, amikor új jelszó létrehozására kényszerítik és a régi jelszó újra használatát nem teszik a

jelszóbiztonsági beállítások lehetővé. A userek 52%-a használja ugyanazt a jelszavát több különböző rendszerbe történő belépésre is és 13%-uk minden rendszerben ugyanazt a jelszót alkalmazza, csak 35%, aki minden account-jához különböző jelszót vagy jelszószéfet alkalmaz. Azonos jelszó használatának elterjedtségére a támadók is számítanak. A bárhol feltört rendszerekből kiszivárgott jelszavakat kipróbálják máshol is, a sikeres belépés reményében. A próbához ötleteket a social network rendszereken átgondolatlanul megadott információk, social engineering támadások segítségével szerezhetnek. Statisztikák szerint a jelszók újra felhasználása a harmadik legtöbbet kihasznált sérülékenység. A felhasználónév-jelszón alapuló hitelesítésnek a jelszavak kialakítása miatt egyéb sérülékenységi problémái is vannak. Elsősorban az, hogy a legtöbb felhasználó olyan jelszavakat hoz létre, amelyek a potenciálisan hozzáférhető nyilvános adatokon, például születésnap vagy egyéb kapcsolódó személyes kötődéseken alapulnak. A jelszavak leggyakrabban használt feltörési módszerei a következő elveket használják. Brute Force módszer, ahol a támadó szisztematikusan próbálja ki a jelszavak összes lehetséges kombinációját, amíg meg nem találja a megfelelőt. Szótár alapú támadás, amikor a gyakran használt jelszavak vagy szótárból származó szavak listája a hitelesítés megkísérlésére szolgál, azokat végig próbálva a gyenge jelszavak megfejthetők. A hibrid módszernél a támadó egyesíti a brute force és a szótári támadások elemeit. Szisztematikusan próbálja ki a szótári szavak különféle kombinációit, gyakori helyettesítéseket és módosításokat. A következő a már említett hitelesítési adatok kitöltése módszer, ami az ellopott felhasználónevek és jelszavak nagy halmazának használatára támaszkodik. A hackerek a korábbi felhasználónevek és jelszavak kombinációjával próbálkoznak. Nem elhanyagolható pont az oktatási környezet specialitása miatt a jelszavak gépelés közbeni megjegyzése, amikor a hallgató az oktató közelében állva a viszonylag lassan begépelt jelszó karaktereit már tudja lokalizálni. Nem érdemes lekicsinyelni a hallgatók motivációit és képességét az oktatói jelszavak megszerzésére. Sajnos van még egy jelszó sérülékenység, szintén az oktatási környezet körülményei miatt, A nem kellően gondos jelszókezelés, ennek egy klasszikus példája a monitorra ragasztott jelszó, illetve az egyszerűen kitalálható, 1234 jellegű jelszavak. Ebben a környezetben az is gyakori lehet, hogy a közösen használt termekben a kurzusok váltásakor az oktató bejelentkezve marad valamilyen fiókjával és szünetben a hallgatók ehhez a számítógéphez hozzá tudnak esetleg férni session eltérítéses támadással vagy akár az operációs rendszer által mentett jelszavak megkeresésével. Az eddigi információk alapján valami hasonló történhetett az eKrétás-s és a több Neptun feltörés esetében is. Ahogy a támadások utáni közleményekből kiderült, egyetemenként egy-két felhasználó volt érintett, az ő jelszavukat szerezte meg a támadó. A Neptun használatánál még könnyíti a jelszó feltöréses támadásokat, hogy a hallgatók és néhol az oktatók felhasználói neve a neptun kódjuk, amelyet nagyon sok helyen használnak, így ki sem kell találni. Ezeket az érzékeny adatokat véleményünk szerint nagyon elővigyázatossággal kellene a felhasználóknak és az oktatási intézményeknek is kezelniük.

A következő adatok is el kell, hogy gondolkoztassanak. Egy hacker 22 másodperc alatt 2,18 billió jelszó és felhasználónév kombinációval tud próbálkozni. Egy nyolc karakteres jelszó feltörése egy másodpercen belül sikerülhet. Ez az idő 22 percre nőhet a kiválasztott jelszóban nagybetű hozzáadásával. A speciális karakterek használata a jelszóban nagyságrendekkel tovább növelheti a feltöréshez átlagosan szükséges időt. A brute force módszer használatának akadályozására azért már az IT biztonságban több kidolgozott módszer található, amelyet az egyetemek többsége is használ, például a meghatározott számú rosszul beütött jelszó utáni megadott időtartamra történő kitiltás, amelyet az idő lejárta előtt csak a megfelelő jogkörrel rendelkező rendszerüzemeltető tud személyes kérés után feloldani. Sajnos, a többi módszer ellen kevesebb gyakorlati védekezési lehetőség áll rendelkezésre. Alapvetően ismert tény a IT és hálózat biztonságban, hogy egy rendszer annyira biztonságos, mint a leggyengébb láncszeme és a biztonságnak a leggyengébb pontja a felhasználó. Ezen nagyon átgondolt és már a korai tanulmányokban elkezdett edukáció tudna segíteni. Ennek sajnos az új Digitális kultúra tantárgy tanterveiben megfelelően átgondolt nyomait se lehet felfedezni. Megmaradó lehetőség az oktatók megfelelő informatikai biztonsági képzésének lehetősége és nagyon pontosan átgondolt információbiztonsági szabályzatok kidolgozása és szigorú, szankciókat is tartalmazó betartatása lenne. Sajnos ennek egyes elemeinek megvalósulása is sok kihívással és nehézséggel küszködik.

Az egyetemi rendszerek biztonságát a látott támadási vektorok alapján mindenképpen erősíteni szükséges. Még több, választékos módszer módszerrel elkövetett támadási próbálkozás is várható, azt előre vetíti az a tény is, hogy a Neptunt működtető szoftver kódbázisának egy része a hacker társadalom és bárki más kezébe került. Többféle tagadást is nyilvánosságra hoztak ebben az ügyben, a teljes tagadástól kezdve, hogy nem szivárgott ki semmi, addig, hogy a letöltésre került kód csak egy régi elavult verzió, amelynek semmiféle relevanciája sincs a ma működő kód esetében. Aki akarta és letöltötte a nyilvános felületen elérhetővé tett kódot és rendelkezett ehhez használható programozói alaptudással az két dolgot mindenképpen észre kellett, hogy vegyen a megszerzett program forráskódjával kapcsolatban. Az első az, hogy még felületesen áttekintve sem nagyon régi és elavult kódnak tűnt. A második az még inkább gondot ébresztő. Az, hogy a kód szerkezete és működési logikája, valamint egyes részletek arra utalnak, hogy nem igazán minőségi és jól struktúrát, jól átgondolt kódot lát a programozó maga előtt. Az informatikusok között ennél sokkal durvább vélemények is megfogalmazódtak és egyetértésre találtak. Volt már olyan eset az informatikai történelemben, amikor rendszerek teljes kódját sikerült a hackereknek letölteni. Van egy híres pozitív példa is, amikor a Cisco IOS teljes kódját szerezték és töltötték át egy orosz szerverre a Cisco hálózati rendszerét sikeresen támadók. Akkor több informatikai szakértő vészhelyzetet kongatott, főleg a gerincvonalak routereinek így lehetővé vált támadása miatt. Akkor és azóta ez a támadás teljes egészében elmaradt, amelyet a szakértők egy jó része az IOS kódjának kiváló minőségének és megbízhatóságának tulajdonított, valószínűleg teljes joggal. Ami akkoriban nagyon megemelte a Cisco hálózati

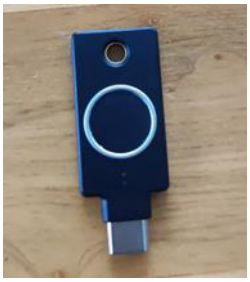
hardverek marketing értékét és elterjedtségét. Sajnos a kód kiszivárgások jelentős része nem végződött ilyen pozitívan és nagy mennyiségű nulla napi sérülékenység alapját szolgáltatta. Ebben az Neptun esetben is a kód minősége alapján erre a kimenetelre van inkább esély. Többen rámutattak a szakértők között, hogy mennyire nem volt szerencsés a középiskolai oktatásban használt eKRÉTA rendszert a Neptun kódbázisán létrehozni és ugyanazokat a fejlesztőket és üzemeltetőket megbízni mindkét rendszer fejlesztésével és működtetésével. A középiskolák egészen más biztonsági szférában tudnak működni, sokkal több és még kevésbé biztonságtudatos felhasználóval, amelyben a tanárokon és a diákokon kívül a szülők is beletartoznak. A középiskolai rendszereket működtető informatikusok sem kellően felkészültek gyakran a biztonsági problémákra adandó válaszokból. Valamint nagyon nem szabad lebecsülni a 15-18 éves korosztály informatikai érdeklődését, az oktatási rendszeren kívül összegyűjtött informatikai tudását és az erős motivációját az adminisztrációra használt rendszer feltörésére és a benne lévő adatok, jegyek, hiányzások és más tények módosítására. Erre sajnos több esetben is fény derült középfokú oktatási intézményekben. Volt, ahol még anyagi bevételt is eszközöltek fiatalok az említett adatok másik számára történő módosításából. A Neptun és az eKRÉTA rendszerének összekötése pont azért is problémás, mert a közös kódbázis kiszivárgása, amely megelőzte az egyetemek Neptun rendszereinek feltörését, egy vagy több egészen fiatal diák támadása miatt következett be. 2022. szeptember 18.-ához kötve az eseményeket. A törésről több, egymásnak ellentmondó adat szivárgott ki. A felelősök sajnos nem a helyzet tisztázását és teljes körű feltárását választották, ami talán segíthetett volna a lehetséges károk mérséklésében. Ehelyett ködösítéssel, a helyzet leértékelésével és erős tagadással kommunikálták a történteket, amivel csak eszkalálták a problémát. Amit alapvetően tudni lehet és sajnos erősíti a céggel kapcsolatos kételyeinket, hogy az egyik projekt vezetője kattintott egy adathalász email linkjére, amivel a támadók megszerezték a belépési adatait, melyekkel aztán hozzáférhettek a belső adatbázisokhoz. A támadással egy 13 éves és egy 15 éves diákot gyanúsítottak. Nem szeretnénk egyik oldalra sem állni, így nem adunk meg hivatkozásokat a történtekkel kapcsolatban. Internetes keresés alapján ki lehet alakítani a saját véleményt a történtekkel kapcsolatban és a dolgok igazán lényegi információi pedig egy Telegram csatornán keresztül kerültek ki, ahogy a forráskód kiszivárogtatása is ott történt. Azért bármelyik oldallal szembeni elfogultság nélkül, mégis kellő megrettenéssel idézzük az oktatást is felügyelő belügyminiszter nyilatkozatát a problémával kapcsolatban: Pénteken Pintér Sándor azt mondta róluk (a fiatal támadókról): „Azért itt vannak tehetségek. Itt volt a KRÉTA rendszernek a feltörése. Nem fogják elhinni, maguk még nem tudják az eredményt. Egy 13 éves és egy 15 éves gyerek törte föl. Tehát van azért jó képzés, van jó példa.” [3]

2 Kétfaktoros azonosítás lehetősége

Az egyetemi Neptun rendszerek és egyéb kiszolgáló rendszerek biztonságának erősítése az eddigiek alapján elengedhetetlen. Mivel a sikeres támadások döntő része a jelszavak megszerzése alapján történt, a jelszavas hitelesítést erősíteni kell. [4] Sajnos nem elégséges bár szükséges a hallgatók és főleg az oktatók edukálása a jelszóbiztonsági szabályok ismeretére és szigorú betartására, de napjainkban ez már biztosan nem elég. A megoldást a két vagy több faktoros autentikáció (MFA) bevezetése jelentheti. A két faktoros autentikáció (2FA) egy hozzáférés-kezelési biztonsági módszer, amely kétféle azonosítást igényel az erőforrások és az adatok eléréséhez. A felhasználó nevet és a jelszót elkérő rendszer, weblap vagy alkalmazás elkér még valami mást is, amivel bizonyítható, hogy valaki hiteles felhasználója a rendszernek. Ilyen például a Netbankok esetében gyakran használt régi ugrókód rendszer, amikor sms-ben jött egy megerősítő kód, amelyet a felületen be kell írni. Ilyenkor nem a kód a lényeg, az valójában annak bizonyítására szolgál, hogy a telefon annak a tulajdonában van, aki az adott műveletet kezdeményezte. Sajnálatos módon ennek a módszernek a feltörésére is vannak a támadóknak sikeres próbálkozásai. Az SMS küldésének ezen kívül anyagi vonzata is van. Gyakran használt megoldás még az ugrókódos rendszer hibáinak javítására egy hitelesítő alkalmazás, autentikátor használata. Ebben az esetben a felhasználó név és jelszó megadása után el kell indítani az autentikátor app-t a rendszernek megadott telefonon és az ott generált hatszámjegyű kódot, amit az app percenként megváltoztat és kiír, be kell írni az alkalmazásba. Ez a kód minden telefonon más, azt hitelesíti, hogy a telefon a hitelesítő személy tulajdonában van. Lehet kód mentes megoldást is alkalmazni, ahol csak el kell fogadni a telefonra érkező értesítést. Ilyen autentikátor app-os 2FA-t már van egyetem, ahol használnak is a belépés biztonságának növelésére. Sajnálatosan ez a módszer is több problémával terhelt, bár kétségkívül hatalmas előrelépés a kizárólag jelszó alapú hitelesítéshez képest. Először is kényelmetlen lehet egy oktatási környezetben oktatók között, hogy a telefonnak is ott kell lennie és elő kell venni és valószínűleg a telefonon is le kell játszani még egy hitelesítési folyamatot. Ha a telefont elfelejtette az oktató a tanterembe magával vinni vagy esetleg a tanterembe felejti óra végén, vagy másutt elveszti a telefont, esetleg telefonszámot cserél, mindegyik az adott pillanatban megoldhatatlanná teszi a hitelesítést. Ráadásul ez a módszer megint függ az egyes felhasználók saját telefonunkon használt hitelesítési módszerének biztonságától is.

Azt a 2FA azonosítás bevezetésénél mindenképpen figyelembe kell venni, kényes egyensúlyt kell kialakítani a biztonság és a használhatóság között. Minél nehezebben kihasználható biztonsági rétegeket építenek egy rendszerbe, az annál biztonságosabb, de ha az adott rendszer használója nem, vagy csak nehézségekkel tudja megoldani a használatát, akkor a kijátszásában lesz érdekelt, például ott hagyja a számítógépet belépve a rendszerbe, hogy ne kelljen a számára kényelmetlen azonosítási folyamaton végig mennie, felírja a túl bonyolult jelszót. Sajnos abban is biztosak lehetünk, hogy az oktatók találékonyak lesznek a

rendszer leegyszerűsítésében, ha nem értik meg a bevezetett biztonsági módszerek fontosságát és nem érzik a rendszert használhatónak.
Ezért felmértük egyetemünkön a kollégáink alapvető véleményét a IT biztonság ezen szegmenséről. Ezek a vélemények nagyon hasznosak lehetnek a hitelesítési módszerek kialakítása szempontjából.
Egyetemünkön egy másik hitelesítési feladatnál (belépés a tantermekbe, oktatói helyiségekbe, saját szobákba), nagy elfogadottsága van az eszköz alapú autentikációnak. Senkinek nem okoz gondot, hogy magával kell a kulcstartóján vinnie egy eszközt a helyiségek kinyitásához. Így azt mértük fel, hogy milyen véleménnyel lennének, ha egy eszközt a számítógépekbe való bejelentkezéshez is rá kellene tenniük a kulcskarikájukra. Vagyis a 2FA-hoz a második eszköz egy YubiKey biztonsági usb kulcs lenne. [5]
A YubiKey biztonsági eszköz úgy néz ki, mint egy normál usb pendrive. amely tartalmaz egy lyukat is a kulcskarika vagy karabiner hozzáerősítéséhez. Saját eszközről kép az első és második ábrán látható. Egy vízálló és mechanikailag is ellenálló kisméretű eszköz. Az usb-n kívül csatlakoztatható más interfacekhez is, pl. Lightning az Apple eszközeihez. De működhet akár rövid távolságú vezeték nélküli kommunikáció, NFC technológiával is. Ebben az esetben kisebb lenne az esély az elvesztésére. Képes aszimmetrikus titkosításhoz szükséges kulcsok tárolására is, ezzel akár a teljes jelszó kezelés is helyettesíthető. A FIDO2 szabvány segítségével az Active Directory is beállítható YubiKey alapú hitelesítésre. PGP kezelésére is konfigurálható, amellyel szükség esetén a biztonságos, harmadik fél számára elolvashatatlan üzenetküldés is megvalósítható. Használható MsWindows, MacOS, Linux és Android operációs rendszerek esetében is. Microsoft 365 alkalmazásokat és a felhő alapú szolgáltatások autentikációját is támogatja. Ami igazán kényelmessé teheti az eszköz használatát, az az ujjlenyomat olvasóval ellátott verzió, amely segítségével a valójában 2FA a felhasználó számára egy eseménynek tűnik, amelyhez semmilyen jelszó megjegyzésére sincs szüksége. Bedugja a YubiKey eszközt a számítógépbe és hozzáérinti az ujját.



Ábra 1

Biometrikus azonosítással ellátott Youbkey

Ez nyilván elvesztés esetén vagy ha valaki egy gépben felejti az eszközét, akkor is teljes mértékben megvéd az illegális használat ellen. Volt olyan kolléga, aki az

ujjlenyomat olvasó használatát zavarónak érezte, érdekes módon informatikát oktató is. Nagy ellenérzés esetén lehet használni egy jelszó alapú vagy pin kód alapú YubiKey változatot is esetükben. Ez nyilván egy lépésnyi visszalépés a biztonságban, de még mindig sokszoros biztonságot nyújt az egyfaktoros jelszavas hitelesítéssel szemben. Mivel ilyenkor is csak egy kellően bonyolult jelszó megjegyzése szükséges és a jelszó nem is kell, hogy végig menjen a hálózaton távoli hitelesítés esetében sem. A YubiKey használata csökkenti a rendszerüzemeltetők terheit is, mivel erősen csökkenti a jelszavakhoz kapcsolódó támogatási események számát. Az eszköz vásárlására fordítandó összeg nem jelentős az egyetemek fenntartási költségeivel összevetve. A kulcsok személyre szabott konfigurálása időt igénylő feladat, de később a kevesebb biztonsági esemény miatt ez kiegyenlítődik.

Ábra 2

YoubiKey pinkód alapú

Az első ábrán egy biometrikus azonosítással ellátott YubiKey látható, a másodikon egy 5C NFC YubiKey és egy YubiKey C Bio a csomagolásával együtt.

3 Munkatársi vélemények elemzése a hálózati azonosítással kapcsolatban

Felmértük kollégáink véleményét a hálózati azonosítással kapcsolatban. Google űrlapot használtunk a megkérdezéshez. 7 tanszékvezető kollégának küldtük ki az űrlap linkjét, kérve, hogy továbbítsák az oktatóknak és kértük a segítséget a véleményformáláshoz a kitöltéssel. Karunkon így kb 140 kollégát értünk el, melyre 70 kitöltés érkezett. Három kérdésben a nemre, korra és az informatikával

kapcsolatos végzettségre kérdeztünk rá. Az értékeléshez 5 fokozatú Likert-skálát használtunk, melyben az 1 érték a kérdés teljes elutasítását jellemezte, az 5 érték, a teljes egyetértést. Ezen ismérvek mellett kerestük az összefüggéseket az alábbi 4 kérdés vonatkozásában:

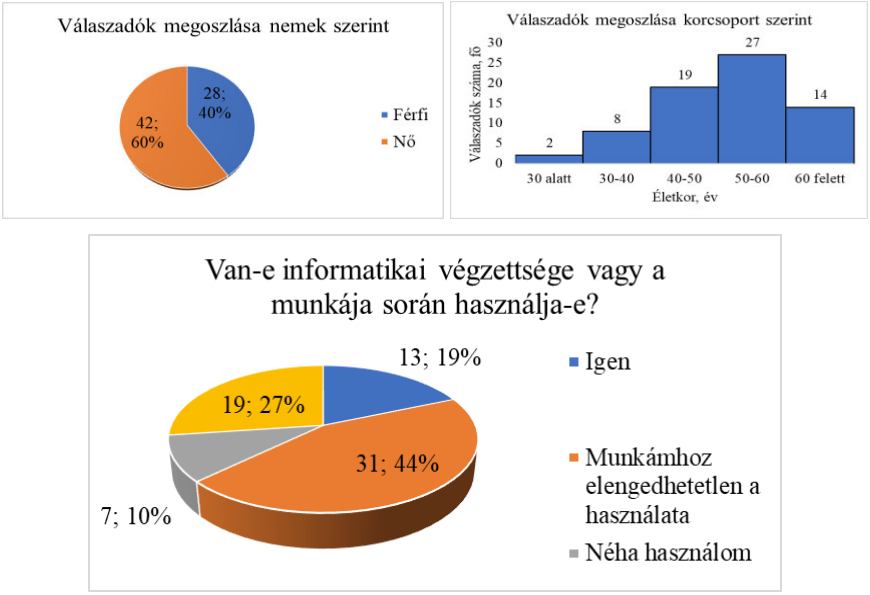
Mennyire ismeri a hálózatoknál használt hitelesítés biztonsági kockázatait?

Mennyire érzi biztonságosnak az egyetemi rendszerek használatához a felhasználói név – jelszó párost?

Mennyire érzi biztonságosnak és nem lenézhetőnek vagy feltörhetőnek a saját használt jelszavát?

Mennyire szívesen használna egy biometrikus (ujjlenyomaton alapuló) azonosítást, ha ahhoz a kicsi, pendrive-szerű eszközt kellene például a kulcskarikáján magánál hordania és használnia és ha elveszíti, akkor sem tudja más felhasználni?

A minta jellemzőit az alábbi grafikonok foglalják össze:



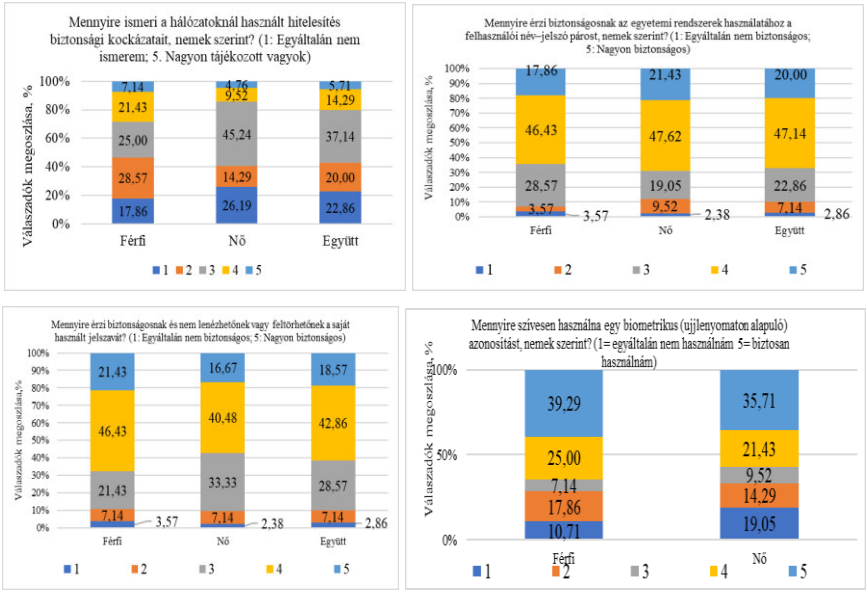
Ábra 3

A minta jellemzőinek összefoglalása

Az egyik szembetűnő adat a válaszadók megoszlása kor szerint: az életkor eltolódott az 50-60 éves korosztály felé. Ezt bizonyítják a számolt adataink is. Az átlagéletkor 51 év, a módusz 54 év, a medián 52 év. Az első kvartilis 44 év, a harmadik 59 év. A számolt F-mutató -0,12153, ami gyenge jobb oldali aszimetriát

jelez. A medián a korcsoport szerinti jellemzésnél fontos, mert így kellett felosztanunk a kor szerinti osztályokat a vizsgálathoz.

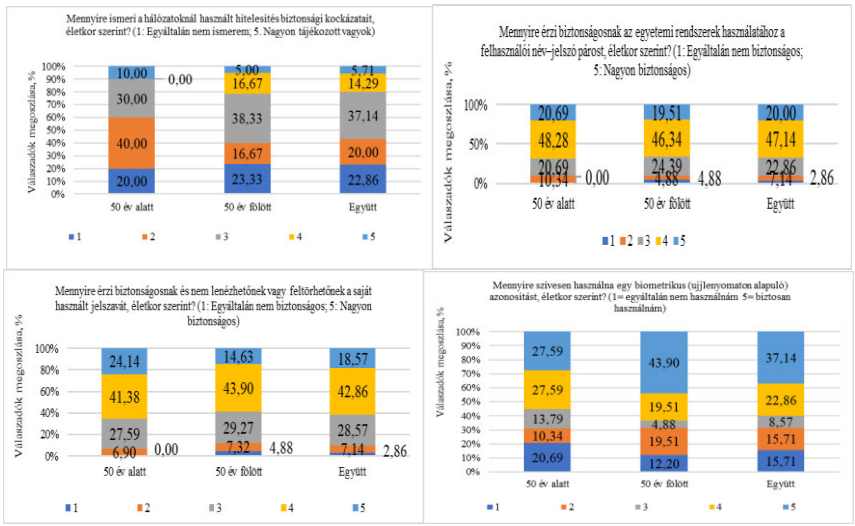
A továbbiakban az egyes kérdések kiértékeléseit mutatjuk be.



Ábra 4

Nemek szerinti adatok az egyes kérdésekre

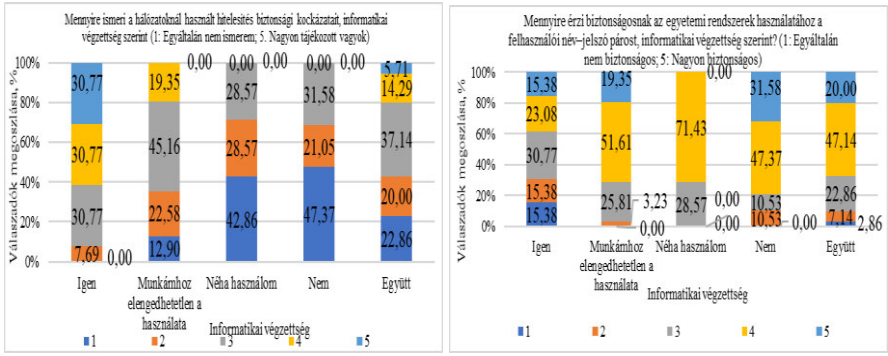
A nők kevésbé ismerik a hálózatoknál használt hitelesítések kockázatait, ugyanakkor az egyetemi rendszereknél használt felhasználói név-jelszó azonosításnál szinte ugyanazokat az eredményeket kapjuk a középzónában, míg a biztonság szempontjából a nők inkább hisznek ebben az azonosítási módban. A férfiak inkább bíznak a saját jelszavaikban mint a nők és ők hajlanak inkább a kétfaktoros azonosításra is.

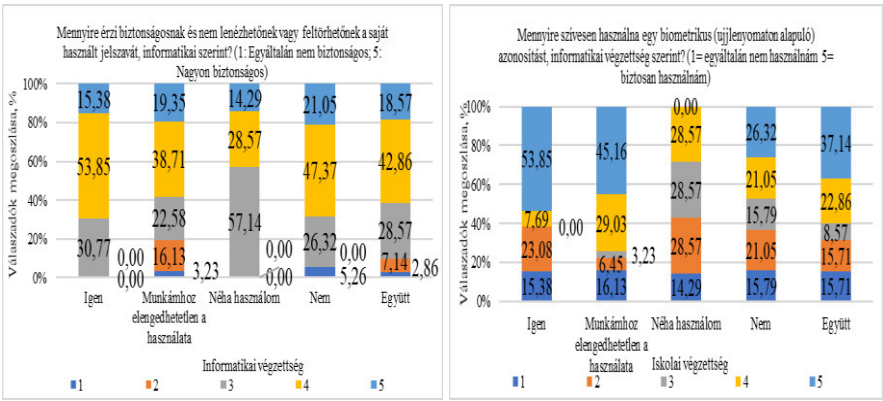


Ábra 5

Hálózati belépés biztonságára jellemző adatok kor szerint

Az 50 év feletti korosztályra jellemzőbb, hogy ismeri a belépési azonosítók használatának és a belépés veszélyeinek kockázatait. A belépési azonosítóikban szinte egyformán biztosak és az 50 év feletti korosztály használná inkább a kétfaktoros azonosítót.





Ábra 6

Iskolai végzettség szerinti adatok ábrázolása

Az informatikai végzettséggel, ismerettel nem rendelkezők kevésbé ismerik a hálózatok hitelesítési biztonsági kockázatát. A munkájukhoz keveset alkalmazó oktatók inkább érzik biztonságosnak az egyetemi rendszerekhez használt azonosítást, mint a rendszeres használók. Az ő esetükben mondható el, hogy a jelszavaikat is biztonságosnak gondolják. Akik néha használják az egyetemi keretrendszereket, elzárkóznak a kétfaktoros azonosítástól, a rendszeres felhasználók és számítástechnikai végzettségűek támogatják a plusz lépés beiktatását.

A négy kérdésünk esetében hipotézisvizsgálatot végeztünk, hogy a három ismérvünk és az egyes kérdések között találunk-e kapcsolatot. Ez mind a négy kérdésünk esetében nem mutatott ki kapcsolatot. Ezt azzal indokoljuk, hogy a mintánk viszonylag kicsinek mondható, így nem mutatható ki a kapcsolat.

Következtetések

Az elmúlt év eseményei is alátámasztják, hogy az egyetemek informatikai rendszerei nagy és egyre növekvő biztonsági nyomás alatt kell, hogy működjenek. Ebben a cikkben végig gondoltuk az egyfaktoros jelszó alapú hitelesítés biztonsági fenyegetéseit és a biztonságosabb jelszó használat követelményeit. Ennek ellenére láttuk, hogy az egyfaktoros autentikáció nem tud megfelelő biztonsági alapokat nyújtani. Ennek ellenére csak két egyetem vezetett be eddig két faktoros hitelesítést az oktatásban használt rendszerekhez. Azt gondoljuk, ennek oka a módszerek kényelmetlensége. Mutattunk egy olyan módszert, amely lényegesen kényelmesebb, ennek ellenére erős hitelesítést tudna nyújtani. Felmértük kollégáink véleményét és azt gondoljuk, hogy a döntéshozóknak meg kellene fontolni a 2FA bevezetését minden egyetemi rendszerben. Ehhez a Neptun fejlesztőinek együttműködése is elengedhetetlen lenne.

Irodalom

[1] Frész Ferenc, Kálovics Tamás, Puha Gábor, Hálózatok Biztonsága, Nemzeti Közszolgálati Egyetem, ÁROP – 2.2.21, 2014

[2] https://www.techopedia.com/cybersecurity-statistics 2023.10.10.

[3] https://444.hu/2022/12/17/egy-15-eves-es-egy-13-eves-fiunal-tartott-hazkutatast-a-rendorseg-a- kreta-rendszer-feltorese-miatt

[4] Kemendi Ágnes: A biztonság hálózata - a kontrollok biztonsági hálózata, https://doi.org/10.14232/jtgf.2022.1-2.77-90

[5] https://yubikey.co.hu 2023.10.15.

[6] Pannon Egyetem Informatikai Szabályzat, https://informatika.uni-pannon.hu/dokumentumok/150-120615-itbizt-ajanlas/file

[7] A Pécsi Tudományegyetem Informatikai Biztonsági Szabályzata, https://adminisztracio.pte.hu/sites/adminisztracio.pte.hu/files/files/Adminisztracio/Szabalyzatok_utasitasok/Hat_Es_Egyeb_Sz/informatikaibiztonsagi_szabalyzat_20220701.pdf

[8] Magyar Testnevelési és Sporttudományi Egyetem Informatikai Biztonsági Szabályzat, https://tf.hu/files/docs/jogiigazgatosag/szabalyzatok/Informatikai_Biztons%C3%A1gi_Szab%C3%A1lyzat_2022-02-01.pdf

[9] Nemzeti Közszolgálati Egyetem Informatikai Biztonsági Szabályzat, https://www.uni-nke.hu/document/uni-nke-hu/informatikai-biztonsagi-szabalyzat_-hataly-2015_-ii_-19-2015_-x_-28_.original.pdf

[10] Budapesti Corvinus Egyetem Informatikai Biztonsági Szabályzat, https://www.uni-corvinus.hu/contents/uploads/2020/02/IT_Informatikai_Biztonsagi_Szabalyzat_v2.1.a93.pdf

[11] Pázmány Péter Katolikus Egyetem Információbiztonsági Szabályzata, https://ppke.hu/storage/tinymce/uploads/old/uploads/articles/34/file/PPKE_Informaciobiztonsagi_Szabalyzat.pdf?u=1axnxo

[12] Szegedi Tudományegyetem Informatikai Biztonsági Szabályzat, https://u-szeged.hu/cc/szabalyzatok

[13] A Budapesti Gazdasági Egyetem informatikai biztonsági szabályzata, https://uni-bge.hu/hu/dokumentumok/22906/szabalyozo-dokumentumok/szenatus-altal-elfogadott-szabalyzatok/informatikai-es-adatvedelmi-szabalyzatok/bge_informatikai-biztonsagi-szabalyzat_20220101.pdf