Felhasználói informatikai biztonsági tudatosság felmérés

Adathalász szimuláció

Készítette: Tóth Attila
Debreceni Egyetem
Információbiztonsági felelős

Kelt: D e b r e c e n, 2025. Január 10.

Tartalom

I. Ok

Releváns kivonat, a 2024. évi LXIX. törvény Magyarország kiberbiztonságáról, 7_2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről, végrehajtási rendeletből.

3.2. Biztonságtudatossági képzés

3.2. A szervezet:

3.2.1. Biztonságtudatossági képzést biztosít a rendszer felhasználói számára (beleértve a vezetőket, felsővezetőket és a szerződéses partnereket is):

3.2.1.1. Az új felhasználók kezdeti képzése keretében, majd ezt követően a szervezet által meghatározott gyakorisággal.

3.2.1.2. Amennyiben az EIR-ben bekövetkezett változások ezt indokolttá teszik, vagy a szervezet által meghatározott események ezt megkövetelik.

3.2.2. Meghatározza azokat a technikákat, melyeket a rendszer felhasználók biztonságtudatosságának növelése érdekében alkalmaz.

3.2.3. Frissíti a képzési és tudatossági tananyagot a szervezet által meghatározott gyakorisággal, valamint a szervezet által meghatározott események bekövetkezését követően.

3.2.4. Integrálja a belső és külső biztonsági eseményekből levont tanulságokat a képzési anyagokba, valamint az alkalmazott biztonságtudatossági eszközrendszerébe

3.3. Biztonságtudatossági képzés – Gyakorlati feladatok

3.3. A szervezet a felkészítő képzést olyan gyakorlati feladatokkal egészíti ki, amelyek szimulálják a biztonsági eseményeket.

3.4. Biztonságtudatossági képzés – Belső fenyegetés

3.4. A szervezet felkészítő képzést nyújt a belső fenyegetések potenciális jeleinek felismerésére és jelentésére.

3.5. Biztonságtudatossági képzés – Pszichológiai befolyásolás és információszerzés

3.5. A szervezet felkészítő képzést nyújt a pszichológiai manipuláció és adatgyűjtés lehetséges és valós jeleinek felismerésére, valamint azok jelentésére.

3.6. Biztonságtudatossági képzés – Gyanús kommunikáció és szokatlan rendszerviselkedés

3.6. A szervezet felkészítő képzést nyújt a szervezet rendszereiben felmerülő gyanús kommunikáció és rendellenes viselkedés felismerésére

3.7. Biztonságtudatossági képzés – Tartós fejlett fenyegetések

3.7. A szervezet felkészítő képzést nyújt a tartós fejlett fenyegetések (APT) felismerésére és kezelésére vonatkozóan.

3.8. Biztonság-tudatossági képzés – Kiberfenyegetési környezet

3.8.1. A szervezet felkészítő képzést nyújt a kiberfenyegetési környezetről és

3.8.2. alkalmazza az aktuális kiberbiztonsági fenyegetési információkat a rendszerüzemeltetésben.

3.9. Szerepkör alapú biztonsági képzés

3.9. A szervezet:

3.9.1. Szerepkör alapú biztonsági képzést nyújt a felhasználóknak:

3.9.1.1. Az EIR-hez vagy az információhoz való hozzáférés engedélyezését vagy a kijelölt feladat végrehajtását megelőzően, továbbá azt követően a szervezet által meghatározott rendszerességgel.

3.9.1.2. Amikor az EIR-ben bekövetkezett változás azt szükségessé teszi.

3.9.2. Frissíti a szerepköralapú képzés tartalmát a szervezet által meghatározott rendszerességgel és a szervezet által meghatározott események bekövetkezését követően.

3.9.3. Beépíti a belső vagy külső biztonsági eseményekből levont tanulságokat a szerepköralapú biztonsági képzésekbe

3.10. Szerepkör alapú biztonsági képzés – Környezeti védelmi intézkedések

3.10. A szervezet kezdeti és időszakos képzést biztosít a szervezet által meghatározott személyek vagy szerepkörök számára a környezethez kapcsolódó biztonsági követelmények alkalmazásáról és működtetéséről.

3.11. Szerepkör alapú biztonsági képzés – Fizikai védelmi intézkedések

3.11. A szervezet kezdeti és időszakos képzést biztosít a szervezet által meghatározott személyeknek vagy szerepköröknek a fizikai biztonsági követelményekből fakadó védelmi intézkedések alkalmazásáról és működtetéséről.

3.12. Szerepkör alapú biztonsági képzés – Gyakorlati feladatok

3.12. A szervezet olyan biztonsági gyakorlati feladatokkal egészíti ki a felkészítő képzést, amelyek megerősítik a képzési célokat.

3.13. A biztonsági képzésre vonatkozó dokumentációk

3.13. A szervezet:

3.13.1. Dokumentálja és nyomon követi az információbiztonsági képzési tevékenységeket, ideértve az általános információbiztonsági tudatossági képzéseket és a speciális szerepkör alapú információbiztonsági

képzéseket.
3.13.2. Meghatározott ideig megőrzi a képzésről készült dokumentumokat.

3.14. Képzés eredményeiről való visszajelzés

3.14. A szervezet rendszeresen visszajelzést ad a meghatározott személyeknek a szervezeti képzések eredményeiről.

II. Cél

A Debreceni Egyetem munkatársainak informatikai tudatossági szintjének felmérése, helyzetviselkedések szimulációs kényszerítésével.

III. Módszer

A Debreceni Egyetem bevezette a kibergyakorlat támogatását szolgáló Awaremon szimulációs rendszert.

Az Awaremon szoftver egy, IT tudatosságot fejlesztő és kiberbiztonsági megoldás, amely számos funkcióval támogatja at Egyetemet, az adathalász támadások és egyéb biztonsági fenyegetések elleni felhasználói tudatosság, felkészültség mérésében.

Fő funkciói

1. Adathalász szimulációk: Automatikusan futtatott adathalász email szimulációk, amelyeket előre gyártott sablonok és testreszabható landing page-ek segítségével hozhat létre. A szimulációk véletlenszerűen küldhetők ki, hogy minimalizálják a felhasználók közötti kommunikáció miatti torzítást.
2. Többnyelvűség: A rendszer és a kampányok nyelve egyszerűen változtatható, igazodva a szervezet igényeihez.
3. Felhasználói szegmentálás: A felhasználók pozíció, tudatosság és egyéb szempontok alapján szegmentálhatók, lehetővé téve a célzott szimulációkat és oktatási anyagok küldését.
4. Automatikus nyelvhez igazított szimulációk: A rendszer automatikusan a felhasználók által használt elsődleges nyelvhez igazítja a szimulációkat, így azok relevánsabbak és hatékonyabbak.
5. Pozíciós kockázat meghatározása: Lehetőség van arra, hogy a felhasználók pozíciói alapján különböző kockázati szinteket állítson be, és ennek megfelelően szabja testre a szimulációkat.
6. Honeypot fiókok létrehozása: Awaremon lehetőséget biztosít honeypot fiókok létrehozására, amelyek segítik az adathalász tevékenységek észlelését.
7. Riasztások valós adathalászat és betörések esetén: A rendszergazdák értesítése valós idejű adathalász támadásokról, integrációval a Microsoft Office rendszerbe.
8. Maszkolás: A személyes adatok védelme érdekében a rendszer nem tárolja a felhasználói adatokat sikeres szimulációk során sem.

9. Automatizált riportálás: Automatikusan generál jelentéseket a szervezet biztonsági állapotáról, melyek időzítése a jogosultsági szintek alapján testre szabható.
10. Onboarding és felhasználói oktatás: Bevezetési folyamat és rendszer használati képzés biztosított, segítve a hatékony használatot.
11. Felhasználói szimulációk automatizált futtatása: A rendszer automatikusan kezeli a felhasználók számára futtatott szimulációkat, a szervezeti struktúrának megfelelően.
12. Előre gyártott sablonok és landing page-ek: Az Awaremon rendszer előre elkészített sablonokat biztosít a gyors kampányindításhoz, amelyeket folyamatosan frissítenek az aktuális adathalász trendekhez igazodva.
13. Kampányok és folyamatok optimalizálása: Automatizált kampányfolyamatok, amelyek testreszabhatók a felhasználói szegmensek és kockázati tényezők alapján. A rendszer randomizálja a szimulációkat, hogy elkerülje a felhasználói közötti előzetes kommunikáció torzító hatását.
14. Microsoft Add-ins: Phishing bejelentő gomb integráció, amely lehetővé teszi a felhasználók számára, hogy gyorsan jelezzék a gyanús e-maileket.
15. Oktatási anyagok és vezetői tájékoztatások: A rendszer képes oktatási anyagokat és vezetői tájékoztatásokat küldeni, monitorozva a felhasználók aktivitását és cselekvési hajlandóságát.

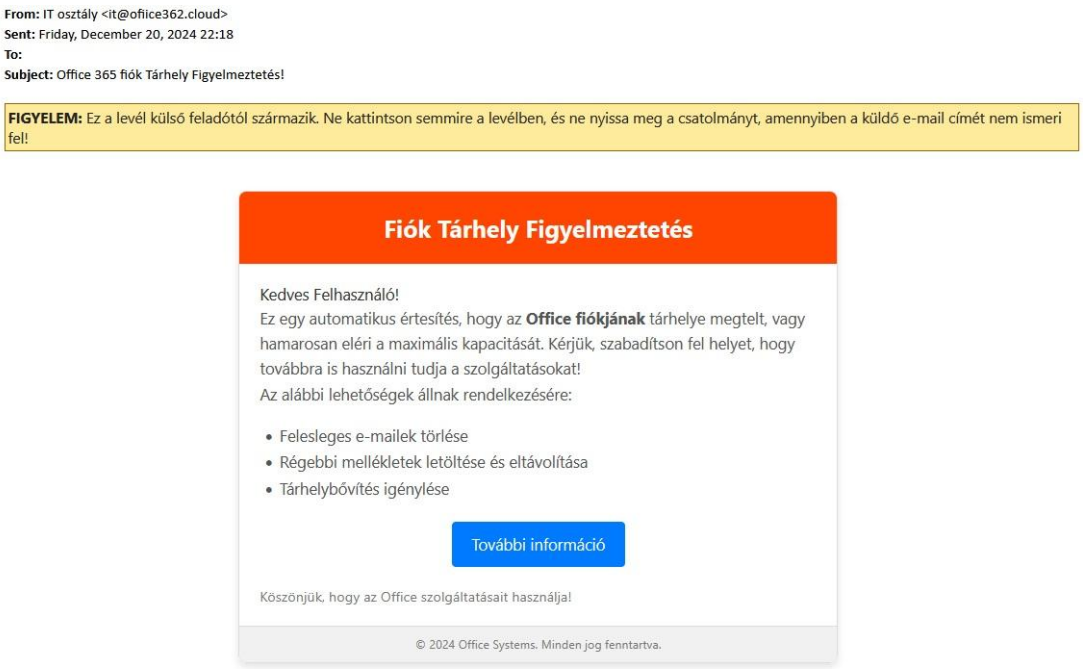
A szimulációs folyamat leírása.

A szimuláció során 3 különböző témájú adathalász tartalmú levelet továbbított a rendszer, az IBK által random kiválasztott 1006 fő munkavállalója részére.

1. Office 365 fiók Tárhely figyelmeztetés
2. Foxpost csomagja megérkezett!
3. Kedvezményes telefonvásár

A szimulációt, az adathalász levelek folyamatos kiköldését, lépcsőzetes időrendiségben eltolva, 2024. November 20-i dátummal indítottuk.

1. Office 365 fiók Tárhely figyelmeztetés



From: IT osztály <it@ofiice362.cloud>
Sent: Friday, December 20, 2024 22:18
To:
Subject: Office 365 fiók Tárhely Figyelmeztetés!

FIGYELEM: Ez a levél külső feladótól származik. Ne kattintson semmire a levélben, és ne nyissa meg a csatolmányt, amennyiben a küldő e-mail címét nem ismeri fel!

Fiók Tárhely Figyelmeztetés

Kedves Felhasználó!
Ez egy automatikus értesítés, hogy az **Office fiókjának** tárhelye megtelt, vagy hamarosan eléri a maximális kapacitását. Kérjük, szabadítson fel helyet, hogy továbbra is használni tudja a szolgáltatásokat!
Az alábbi lehetőségek állnak rendelkezésére:

- Felesleges e-mailek törlése
- Régebbi mellékletek letöltése és eltávolítása
- Tárhelybővítés igénylése

További információ

Köszönjük, hogy az Office szolgáltatásait használja!

© 2024 Office Systems. Minden jog fenntartva.

2. Foxpost csomagja megérkezett!

From: Foxpott levél <fox@newportal.store>
Sent: Friday, December 20, 2024 21:10
To:
Subject: Foxpost csomagja megérkezett!

FIGYELEM: Ez a levél külső feladótól származik. Ne kattintson semmire a levélben, és ne nyissa meg a csatolmányt, amennyiben a küldő e-mail címét nem ismeri fel!

FOXPOST Csomag Értesítés

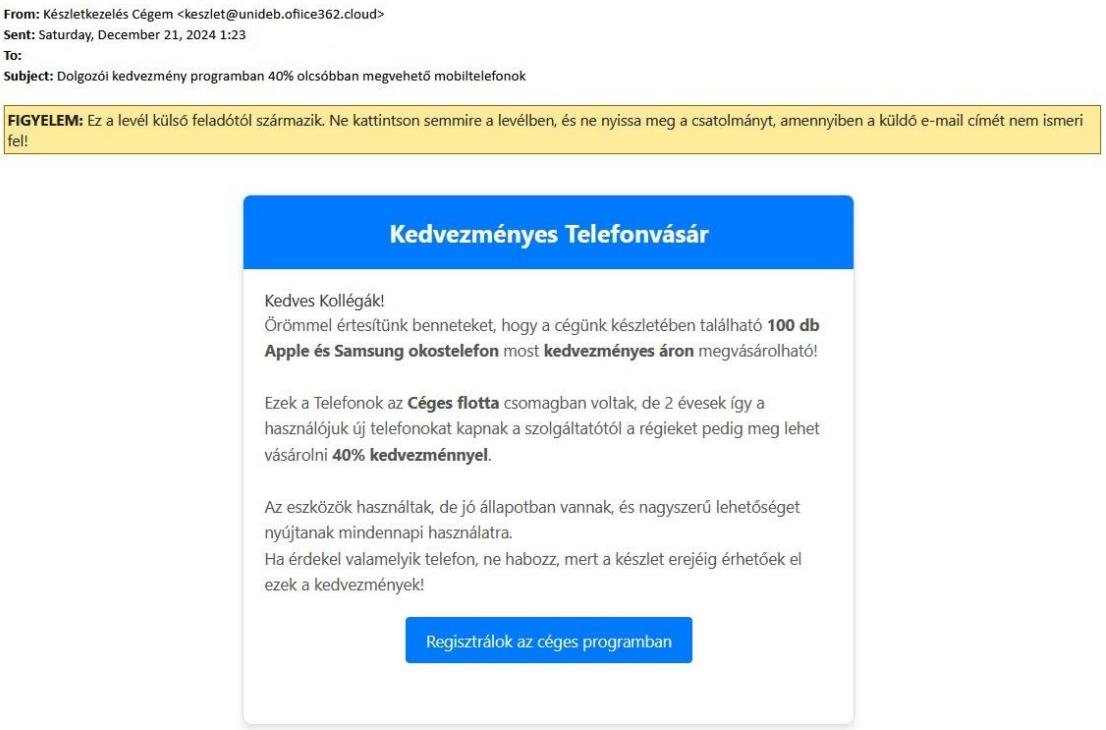
Kedves Ügyfelünk!
Örömmel értesítjük, hogy az Ön csomagja megérkezett az **FOXPOST** csomagautomatába. A pontos átvételi helyszínt és további részleteket az alábbi linken érheti el:

Átvételi hely megtekintése

Kérjük, hogy mielőbb vegye át csomagját, hogy helyet biztosíthassunk a következő küldemények számára. Köszönjük, hogy a FOXPOST szolgáltatását választotta!

© 2024 FOXPOST. Minden jog fenntartva.

3. Kedvezményes telefonvásár



From: Készletkezelés Cégem <keszlet@unideb.ofiice362.cloud>
Sent: Saturday, December 21, 2024 1:23
To:
Subject: Dolgozói kedvezmény programban 40% olcsóbban megvehető mobiltelefonok

FIGYELEM: Ez a levél külső feladótól származik. Ne kattintson semmire a levélben, és ne nyissa meg a csatolmányt, amennyiben a küldő e-mail címét nem ismeri fel!

Kedvezményes Telefonvásár

Kedves Kollégák!
Örömmel értesítünk benneteket, hogy a cégünk készletében található **100 db Apple és Samsung okostelefon** most **kedvezményes áron** megvásárolható!

Ezek a Telefonok az **Céges flotta** csomagban voltak, de 2 évesek így a használójuk új telefonokat kapnak a szolgáltatótól a régieket pedig meg lehet vásárolni **40% kedvezménnyel**.

Az eszközök használtak, de jó állapotban vannak, és nagyszerű lehetőséget nyújtanak mindennapi használatra.
Ha érdekel valamelyik telefon, ne habozz, mert a készlet erejéig érhetőek el ezek a kedvezmények!

Regisztrálok az céges programban

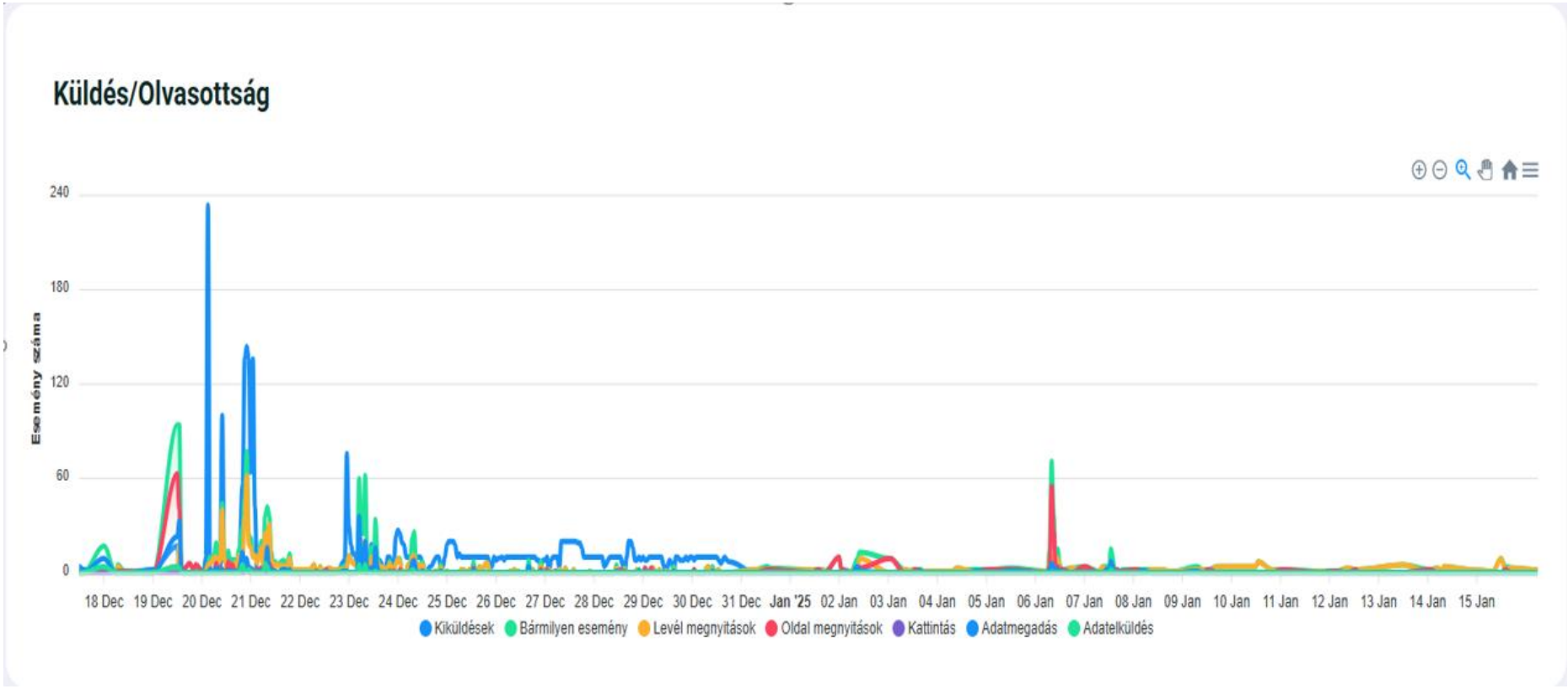
IV. Eszköz

AWAREMON IT tudatosság tesztelő és ellenőrző rendszer

V. Eredmény

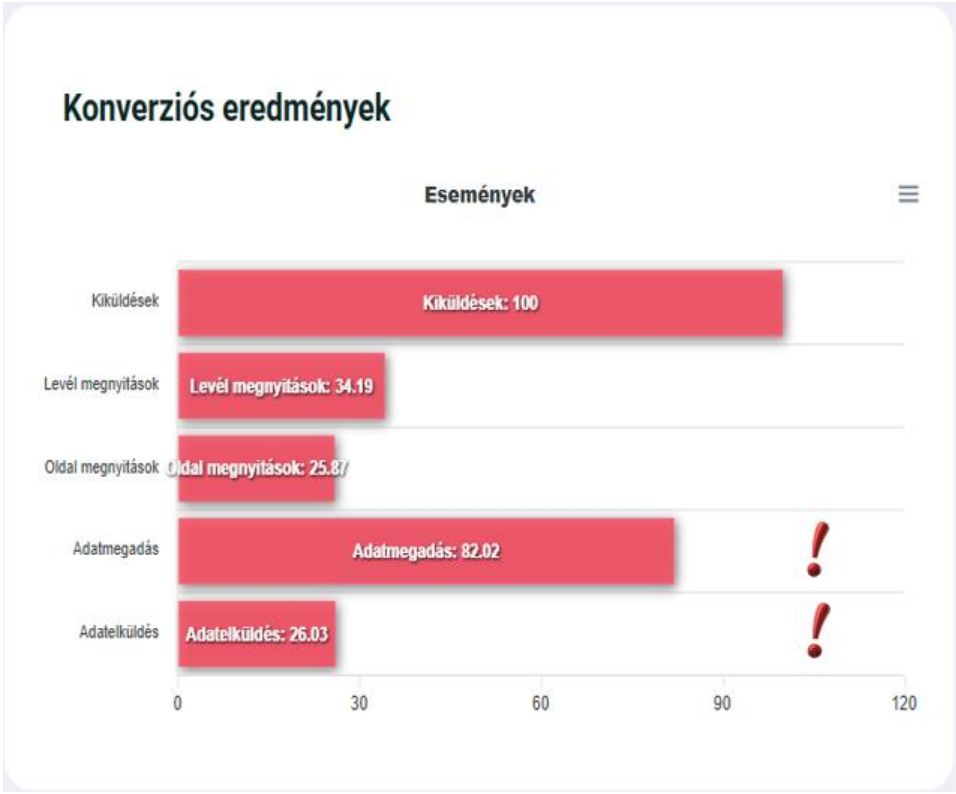
Az adathalász szimulációs kampány eredményének kiértékelése.

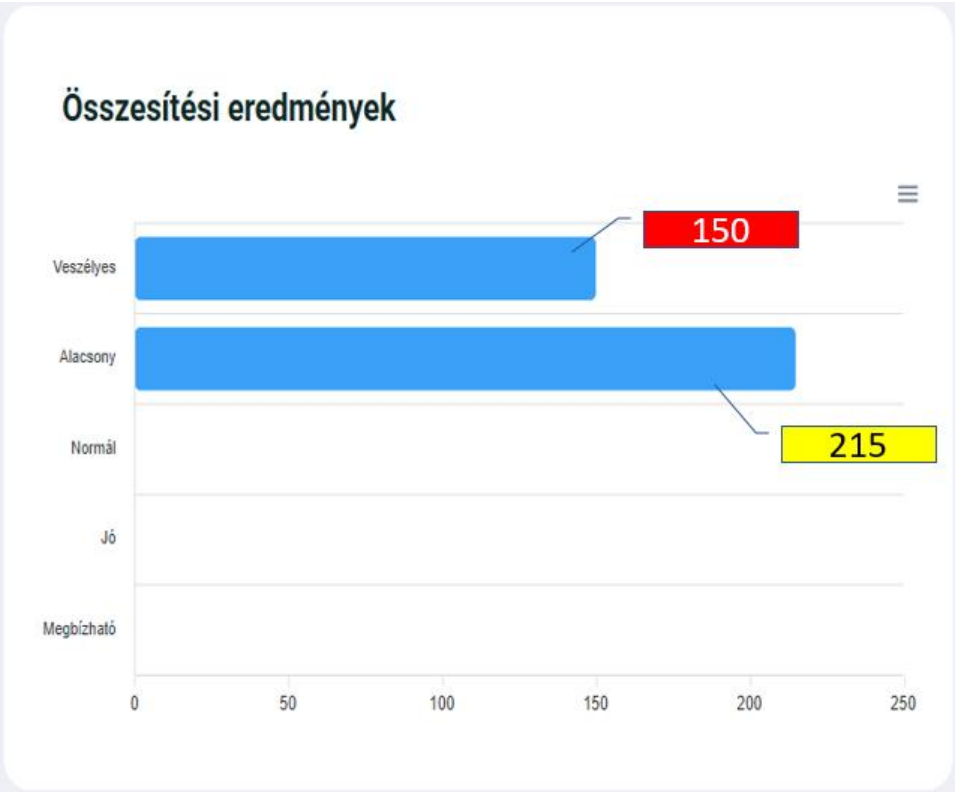
Összesítő statisztikai jelentés



Kockázati konverzió

Neve	Események száma	Személyek száma	%	
Kiküldések	3032	1006	100	Részletek
Levél megnyitások	978	344	34.19	Részletek
Oldal megnyitások	442	89	25.87	Részletek
Adatmegadás	298	73	82.02 !	Részletek
Adatelküldés	48	19	26.03 !	Részletek


Konverziós eredmények
Események
Kiküldések
Levél megnyitások
Oldal megnyitások
Adatmegadás
Adatelküldés
Kiküldések: 100
Levél megnyitások: 34.19
Oldal megnyitások: 25.87
Adatmegadás: 82.02
Adatelküldés: 26.03
0
30
60
90
120


Összesítési eredmények
Veszélyes
Alacsony
Normál
Jó
Megbízható
150
215
0
50
100
150
200
250

VI. Értékelés

Az adathalász kampány elérte a kitűzött célunkat, ugyanis a mintavételi csoport mutatószámai alapján behatárolhatjuk azt a célterületet, amire jobban oda kell fókuszálnunk. Az „Adatmegadás" 82%-a és az „Adatküldés" 26 %-a mutatja, a biztonságtudatosság egyetemi szintjét, ami jelen csoport esetébenalacsonynak minősített Megállapíthatjuk, hogy az általunk publikált tananyagok alacsony megtekintési és elvégzési mutatói, az alacsony részvételi arány, jelen kampányban köszön vissza. A tananyagok vizuálisan szemléltetik, hogy mikor hogyan kell biztonságtudatosan cselekedni, ami jelen szimuláció során hasznos információ lett volna az áldozatul esett munkavállalóknak.

Tudatos információbiztonságot sértő támadás megelőzése és kivédése nem történhet ösztönös viselkedés által, mivel a napjainkban összetett, kifinomult és mesterséges inteligenciával támogatott fejlett kiberbűnözés egy lépéssel előtte halad a védelemnek.

Egy IT bölcselet szerint az informatikai problémák legnagyobb része a billentyűzet és a szék között van.
Az informatikai védelem leggyengébb láncszeme, „AZ EMBER"

- Szakképzetlenség
- Szakszerűtlen üzemeltetés
- Szakszerűtlen karbantartás
- Szándékos károkozás (bosszúállás)
- Eltulajdonítás
- Megvesztegetés
- Szabálytalan kezelés
- Figyelmetlenség, nem odafigyelés
- Hozzáférési előírások tudatos megsértése
- Jóhiszeműség

Ezek kezelése csak biztonságtudatos-, pozitív hozzáállással történhet eredményesen.

A biztonsági tudatosság, az Egyetem kultúrájának része.
Olyan gondolkodás- és magatartásmód, amely biztosítja, hogy a munkatársak személyes elkötelezettségből elismerik a biztonsági intézkedések jogosságát, betartják-, betartatják és másokkal is megismertetik azokat.

Összegzés: A cél, a nem biztonságtudatos viselkedések minimalizása, hogy kiberbűnözők csaló módszerekkel megszerzett adatok birtokában semmilyen módon ne tudjanak az egyetemi infrastruktúrához, információs rendszereihez hozzáférni. A biztonságtudatosság erősítése, célzott és általános

biztonságtudatossági oktatások biztosítása folyamatos tevékenység kell, hogy legyen, amit az Informatikai Biztonsági Központ biztosítani fog.