THE PLACE OF SOCIAL ENGINEERING IN THE INFORMATION SECURITY AUDIT

A SOCIAL ENGINEERING HELYE AZ INFORMÁCIÓBIZTONSÁGI AUDITBAN

BARNA Bianka Rita[1] – KOLLÁR Csaba[2] – OROSZI Eszter Diána[3]

Abstract

In the information security audit, it is possible to use several methods and techniques, in this study we focused on social engineering. After the theoretical parts of the topic (audit, information security audit, expectations of the auditor, the importance of the audit, application of social engineering), we present the structure, process, and public results of an information security audit conducted in a real, large company environment. The name of the company will not be mentioned in our study. Based on the results, we formulate proposals for the development of information security awareness, and we also cover the presentation of the more important awareness development methods.

Keywords

audit, information security audit, social engineering, development of security awareness, case study

Absztrakt

Az információbiztonsági auditban többféle módszer és technika használatára van lehetőség, jelen tanulmányunkban a social engineeringre fókuszáltunk. A téma elméleti részei (audit, információbiztonsági audit, auditorral szembeni elvárások, az audit fontossága, social engineering alkalmazása) után egy valós, nagyvállalati környezetben végzett információbiztonsági audit felépítését, folyamatát, illetve publikus eredményeit mutatjuk be. A vállalat neve kérésére tanulmányunkban nem kerül megemlítésre. Az eredmények ismeretében javaslatokat fogalmazunk meg az információbiztonság-tudatosság fejlesztésére, illetve kitérünk a fontosabb tudatosság fejlesztési módszerek bemutatására is.

Kulcsszavak

audit, információbiztonsági audit, social engineering, biztonságtudatosság fejlesztése, esettanulmány

[1] biankabarna81@gmail.com | ORCID: 0009-0001-9367-3882 | information security technology specialist, Citibank | információtechnológiai biztonsági szakértő, Citibank

[2] kollar.csaba@uni-obuda.hu | ORCID: 0000-0002-0981-2385 | senior research fellow and leader, Óbuda University Bánki Donát Faculty of Mechanical and Safety Engineering Artificial Intelligence Workshop | tudományos főmunkatárs és vezető, Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar Mesterséges Intelligencia Műhely

[3] oroszi.eszter@silentsignal.hu | ORCID: 0000-0001-8048-9034 | Head of Information Security Consulting Department, Silent Signal Ltd. | információbiztonsági tanácsadás üzletágvezető, Silent Signal Kft.

ELMÉLETI ALAPVETÉS

Az audit

Az audit egy olyan ellenőrzési folyamat, mely során különböző eljárások és tesztek alapján kivizsgálják, hogy az adott vállalat bizonyos részei, területei, (tanulmányunkban az információbiztonsági rendszerekben alkalmazott intézkedések) megfelelnek-e az elvárásoknak, mind a vállalat belső, mind a külső szabályozásokra tekintettel. Ezek az ellenőrzések biztosítják a vezetőséget arról, hogy minden folyamat a megfelelő módon történik a vállalatnál. Például ez egy tökéletes lehetőség arra, hogy a vezetés egy tisztább képet kapjon egy pártatlan személytől arról, hogy az alkalmazottak hogyan tartják be a vállalati irányelveket, a szabályozásokat és hogyan tartják magukat a velük szemben támasztott elvárásokhoz. Ugyan így, fény derülhet arra is, ha esetleg a munkatársak sorozatosan hibát követnek el valamely területen. Ilyen lehet például, ha biztonsági adatmentéseket elmulasztják megtenni, vagy ha a vállalat nem megfelelően vezeti a könyvelést. [1]

Egy adott vállalat szinte bármely részét auditálhatják. Az ellenőrzést ott szokták legtöbbször elvégezni, amely területek: magasabb prioritásúak, régen voltak felülvizsgálva vagy épp pont egy új program/ rendszer kerül bevezetésre az adott területen, melyet felül kell vizsgálni a helyes működés érdekében. [2]

Az audit legfontosabb követelménye, a független auditor személye. Ezért alakultak ki olyan széles körben elismert és elfogadott szervezetek, amelyek meghatározzák a követendő szabványokat és szabályokat az auditokat illetően. Ilyenek például az ISACA, az auditorok nemzetközi szakmai szervezete. Szinte minden országban (és államban) megtalálható valamilyen tagszervezete, például Magyarországon is. Az ISACA alapvető célja, hogy az információs rendszereket ellenőrizni és irányítani lehessen egy megadott keretrendszer szerint. [2]

Az auditálásnak több különböző típusa is van, tanulmányunkban elsősorban a belső auditokkal foglalkozunk részletesebben. A belső audit a szervezet saját szabályainak és követelményeinek betartását ellenőrzi. Ezek a felülvizsgálatok megtervezett időközönként ismétlődnek annak érdekében, hogy a vezetőség minél átfogóbb és naprakészebb információkkal bírjon a szervezete működéséről. Miután az időpontot kijelölték, fontos, hogy egy előre elkészített auditprogram szerint dolgozzanak, és megfogalmazzák az audit kritériumokat. Az auditorok kiválasztása is fontos feladat az objektív és teljesen pártatlan véleményformálás miatt. Ha a vizsgálatokat lefolytatták, az audit eredményeket jelentik a vezetésnek, és ha vannak, akkor a szükséges helyesbítéseket is végre hajtják. Ezután egy hivatalos dokumentumként az auditprogram és az audit eredményei megőrzendők. [1][2]

Az információbiztonsági audit

Az információbiztonsági auditok ugyan úgy lehetnek belső és külső auditok is. Ebben az esetben a belső információbiztonsági auditok néhány jellemzőjét ismertetjük. Ezeket az auditokat egy kiválasztott személy folytatja le, mely a szervezet egyik saját alkalmazottja, vagy egy a szervezet által megbízott alvállalkozó. Ezen auditok célja a lehetséges jövőbeli fejlesztések megismerése, és a követelményeknek való megfelelések vagy épp nem megfelelőségek észrevétele. Az eredményük pedig, egy auditjelentés mely részletesen ismerteti a megfelelőségeket, (vagy azok hiányát) és akár javaslatot is tehet a fejlesztési tervekhez és egyéb intézkedésekhez. Általában az ilyen auditok évente követik egymást. Ezek

ekkor teljeskörű vizsgálatot jelentenek, azonban lehetséges soron kívüli auditot is indítani. (Erre indok lehet például egy új jogosultságkezelő program használatba vétele a vállalatnál.) [2]

Minden belső audit a rá vonatkozó ISO szabványt, esetleg egy partner vállalt követelményeit, illetve az adott intézmény saját, belső követelményeit és elvárásait követi. Az információbiztonságra vonatkozó legismertebb szabvány melyet egy kissé bővebben ismertetünk, az MSZ ISO/IEC 27001:2014 [12].

Az ISO/IEC 27001:2014, a szabvány mai napig Magyarországon hatályos kiadása. A legújabb kiadást 2022 októberében publikálták, azonban hazánkban a honosítás miatt jelenleg is a 2014-es változatot használták a tanulmány készítésének időszakában. [3]

A legtöbb szervezet komoly struktúrát igényel, ha az információbiztonságról és annak ellenőrzéséről van szó. Az ISO/IEC 27001 erre ad megoldást, hiszen gyakran ad megoldás konkrét helyzetekre, és ez alapján majdnem felépíthető egy vállalat Információbiztonsági Irányítási Rendszere (IBIR). A benne szereplő ellenőrzések leginkább az IT (információtechnológia) és az adatbiztonság témakörét öleli fel, azonban a nem IT vonatkozású eszközök (ahogy a papírmunka és a védett nyomtatványok) kevésbé kerültek kidolgozásra, így kevésbé védettek. [2]

A vállalati vezetés meghatározhatja az IBIR hatáskörét és akár egyetlen egy helyszínre vagy üzleti egységre is korlátozhatja azt [6] [7]. Ezért, ha ismert, hogy egy szervezet egy bizonyos részen alkalmazza az ISO/IEC 27001-et, az nem jelenti az, hogy kijelenthető, a vállalat egyöntetűen megfelelést vár el ehhez a szabványhoz képest. Az ISO/IEC 27000-es szabványcsalád a többi elemével együtt további útmutatást adnak az IBIR tervezéséhez, megvalósításához és a működtetési szempontokhoz. [2]

A szabvány legfontosabb része az „A melléklet”, mely a következő kérdésekre ad útmutatást [12]:

„A5. Információbiztonsági szabályok
A5.1. Az információbiztonság vezetői irányítása
A6. Az információbiztonság szervezete
A6.1. Belső szervezet
A6.2. Mobil eszközök és távmunka
A7. Az emberi erőforrások biztonsága
A7.1. A munkaviszony kezdte előtt
A7.2. A munkaviszony fennállása során
A7.3. A munkaviszony megszűnése és megváltozása
A8. Vagyonelemek kezelése
A8.1. A vagyonelemekért viselt felelősség
A8.2. Információosztályozás
A8.3. Adathordozók kezelése
A9. Hozzáférés-felügyelet
A9.1. A hozzáférés-felügyelettel kapcsolatos üzleti követelmények
A9.2. A felhasználói hozzáférések kezelése
A9.3. Felhasználói felelősségek
A9.4 Rendszer- és alkalmazás-hozzáférés felügyelete
A10. Titkosítás
A10.1 Titkosítási intézkedések

A11. Fizikai és környezeti biztonság
A11.1 Biztonsági területek
A11.2. Berendezés
A12. Az üzemeltetés biztonsága
A12.1. Üzemeltetési eljárások és felelősségek
A12.2. Védelem a rosszindulatú szoftverek ellen
A12.3. Mentés
A12.4. Naplózás és megfigyelés
A12.5. Az üzemeltető szoftverek felügyelete
A12.6. A műszaki sebezhetőségek felügyelete
A12.7 Az információs rendszerek auditálásával kapcsolatos megfontolások
A13. A kommunikáció biztonsága
A13.1. A hálózatbiztonság biztosítása
A13.2. Információátvitel
A14. Rendszerek beszerzése, fejlesztése és karbantartása
A14.1. Az információs rendszerek biztonsági követelményei
A14.2. Biztonság a fejlesztési és támogatási folyamatban
A14.3. Tesztadatok
A15. Szállítói kapcsolatok
A15.1 Információbiztonság a szállítói kapcsolatokban
A15.2. A szállítói szolgáltatásnyújtás irányítása
A16. Az információbiztonsági incidensek kezelése
A16.1. Az információbiztonsági incidensek és javítások kezelése
A17. A működésfolytonosság biztosításának információbiztonsági vonatkozásai
A17.1. Az információbiztonság folytonossága
A17.2. Tartalékok
A18. Megfelelés
A18.1. Megfelelés a jogi szerződéses követelményeknek
A18.2. Információbiztonsági vizsgálatok”

Ezen szempontok alapján tanúsítják a vállalatokat, és írja meg sok vállalat az IBIR-t.

Az auditorral szemben elvárt követelmények

Egy audit előkészítésekor fontos, hogy az auditor megfelelő kapcsolatot tartson az auditáltakkal. Ezzel biztosítja, hogy a lehető legjobban az adott vállalathoz viszonyítva ellenőriz. Így pontosítja az elvárásokat az összes résztvevő között, mely többek között magában foglalja a releváns információkat az audit célját illetően, a vizsgálat hatásköréről és kritériumairól, az alkalmazott módszerekről és az ellenőrzési csoport összetételéről is. Az auditor a legtöbb esetben hozzáférést kér az audithoz szükséges releváns információkhoz, melyek tartalmazzák a szervezet által meghatározott kockázatokat, valamint azok kezelését is. [1][2]

Az auditornak felül kell vizsgálnia az auditált vállalat irányítási rendszerének dokumentációit. Ezeknek tartalmaznia kell az irányítási rendszer korábbi audit jelentéseit, saját dokumentumait. Erre azért van szükség, hogy a releváns információkat összegyűjthesse,

és készítsen saját részére egy áttekintést, a lehetséges megfelelések, vagy épp nem megfelelések előre vetítése érdekében. A felülvizsgálatot követően meg kell tervezni az auditot. Ez segít betartani az ütemtervet és a tevékenységek összehangolását. [4]

Az auditornak külön figyelmet kell fordítania arra, hogy a terv elkészítésének folyamata, a terv tartalma eltérhet különböző külső tényezők miatt. Ilyen lehet például, ha vannak már megelőző auditokról feljegyzések, vagy ha épp ez az első. Illetve az is számít, hogy külső, avagy belső auditról van szó. Egyéb előreláthatatlan okok miatt az elkészült tervezetnek elég rugalmasnak kell lennie ahhoz, hogy a később, a felülvizsgálat előrehaladtával felmerülő változásokat eszközölni lehessen. [4]

Azonban az auditornak nem csak tankönyvekben meghatározott elvárásoknak kell megfelelnie. Az ő helyzetében nagyon fontos az is, hogy megfelelő első benyomást tegyen és a lehető legszimpatikusabban (de határozottan) prezentálja magát az auditáltak előtt. Ilyenkor döntő szerepet játszik a külső megjelenés, valamint a helyes verbális és nonverbális kommunikáció alkalmazása. A folyamatos jelenlét, a lelkes munkavégzés és a szakmai jártasság egyaránt fontosak ahhoz, hogy a felülvizsgálatot végző személy a vállalat minden területén megfelelő kapcsolatot tudjon kialakítani az auditáltakkal.[2][4]

Információbiztonsági audit fontossága

Az információbiztonsági audit fontossága véleményem szerint az összetettségében rejlik. Ekkor az auditor nem csak a vállalat folyamatait kell megfigyelje, de betekintést nyer a munkatársak biztonság-tudatosságába is a mindennapokban. Ezt az összetettséget nagyon jól szemlélteti Baglyos írása:

„Az információbiztonsági audit a szervezetek informatikai infrastruktúrájának átfogó felülvizsgálatát jelenti. Ezek a fajta auditok biztosítják, hogy a megfelelő irányelveknek, eljárásoknak, jogszabályoknak eleget tettek és ezáltal hatékonyan működnek. A vizsgálatok célja, hogy olyan sebezhető pontokat azonosítsanak, amelyek adatvédelmi incidenseket idézhetnek elő. Ezek lehetnek azok a sebezhetőségek, amelyeket a támadók kihasználhatnak a jogosulatlan hozzáféréshez. Az információbiztonsági audit elvégzésének fő oka a biztonsági és megfelelőségi hiányosságok azonosítása, valamint azok kezelése. Egy alapos felméréssel a szervezet átfogó képet kaphat a rendszereiről, és betekintést nyerhet a sebezhetőségek kezelésének legjobb módszereibe. A szervezeteknek nem csak az üzleti tevékenység megszakadásának és a hatósági bírságoknak a veszélye miatt kell aggódniuk, mivel egy biztonsági incidens (különösen, ha az megelőzhető lett volna a megfeleléseknek eleget téve) valószínűleg a beszállítók és az ügyfelek bizalmát is csökkentheti. Ha az incidens elég súlyos volt, ezek az érdekeltek akár úgy is dönthetnek, hogy nem kívánnak továbbra is együtt dolgozni az adott szervezettel. Ugyanez vonatkozik a szabályozási hibákra is. Ha a szervezet bizonyítani tudja, hogy megfelelő lépéseket tett az adatvédelemmel kapcsolatban, a szabályozó hatóságok nem fognak jelentős bírságokat kiszabni. Ha azonban az incidens gondatlanságból következett be, a szervezetekre súlyosabb büntetések várhatnak. Ha ezek a büntetések nem is közelítik meg a GDPR által megengedett maximumot (20 millió euró vagy a szervezet éves globális forgalmának 4%-a), egy viszonylag enyhe bírság is katasztrofális lehet a szervezet jövőjére nézve.

Az információbiztonsági audit során az eddig említetteken túl, vizsgálják még:

- az adatbiztonságot: hálózati hozzáférés, adattitkosítás;
- a működési biztonságot: irányelvek, eljárások, ellenőrzések;

- a hálózati biztonságot: vírusvédelem, hálózatfelügyelet;
- a rendszerbiztonságot: javítás, privilegizált fiókok kezelés;
- valamint a fizikai biztonságit: külső, belső területvédelem, eszközök, vagyontárgyak védelme." [5]

Ebben a cikkben a szerző referál a 2013. évi L. törvényre, mely hazai viszonylatban igen meghatározó, a vállalatok adatvédelmi, információbiztonsági struktúráinak kialakításakor. Ezért is annyira fontos a helyes információbiztonsági auditálás, mivel ez a törvény olyan elengedhetetlen pontokat érint, mint a biztonsági események kezelése; biztonsági osztályba sorolás; védelem kialakítása; stb.

Az említett pontok által világosan látszik az információbiztonsági audit relevanciája. Összességében, az információbiztonsági audit segít betartani a szabványokat és jogszabályokban meghatározott előírásokat, valamint bepillantást enged a vállalat információbiztonsági szemléletébe.

A social engineering alkalmazása az audit során

Az információbiztonság világában igyekszünk lehető legkevesebb támadási felületet hagyni a támadók számára. Azonban amíg az online világban több lehetőségünk is van az esetleges támadások kivédésére, (akár egy vírusírtó segítségével, egy tűzfallal vagy néhány korlátozás bevezetésével) a valóságban létezik egy olyan biztonsági rés, melyet bárki, bármelyik adandó pillanatban kihasználhat. Ez pedig nem más, mint az a tény, hogy a munkatársak bizony „csak" emberek.

Mivel a social engineering számos technikával kivitelezhető [11] a munkatársak felkészítése egy ilyen esetre sokkal nehezebb. Azonban, ha egy auditba építve számon tudják kérni a vállalatot, az rá lesz kényszerítve arra, hogy megfelelően „bizalmatlanná" tegyék a munkatársakat, ezzel felkészítve őket egy esetleges social engineering támadásra.

Egy megfelelően kidolgozott kötelező információbiztonság-tudatossági oktatással, amely meghatározott időnként megismétlésre kerül, jól szinten tartható a kellő óvatosság a munkatársak körében.

A TÉMA EMPIRIKUS VIZSGÁLATA

A következőkben esettanulmányként egy nagyvállalatnál végzett információbiztonsági auditot és annak eredményeit ismertetjük.

A vállalati környezet ismertetése

Az adathalász kampányt nagyvállalati környezetben végeztük. Az energiaszektor egyik kiemelt szereplőjeként a cég nagy figyelmet fordít a biztonságra. Ahhoz, hogy a megfelelő információbiztonság-tudatossági oktatást biztosíthassák munkavállalóik számára, fontos, hogy mindig naprakész adataik legyenek arról, milyen a vállalat általános teljesítménye egy éles helyzetben.

A vállalatnak több telephelye is van, a fővárosban és az ország minden területén egyaránt. Ahogy az majd később az adathalász e-mail eredményeiben is megmutatkozik, jelenleg 6946 munkavállaló dolgozik összesen a vállalat telephelyein. Ez a szervezet követi a tipikus nemzetközi nagyvállalatok felépítését. Megkülönböztet vezérigazgatót és -helyetteseket, valamint igazgatóságot és osztályokat (ezeken belül néha csoportokat) is. Ezek a

jól elválasztott rétegek, gyakran még inkább megkönnyítik az adathalászok dolgát, hiszen egy kevés utánajárás után (például LinkedIn segítségével) könnyen találhat a céljainak megfelelő áldozatot, akire a támadást irányítani fogja. Az általában a legjobban veszélynek kitett pozíciók közül néhány példa lehet: a vezérigazgatóság tagjai, az üzemeltetés vagy a kontrolling tagjai, bármilyen humánpolitikai vonatkozású beosztás, vagy akár a kommunikációs munkatársak, hiszen ők még szorosabb kapcsolatban vannak a közösségi oldalakkal és a sajtóval.

A vállalaton belül kiforrott intézkedések működnek egy esetleges adathalász kampány bekövetkeztének esetére. Egyaránt használnak spam-szűrőket, tűzfalakat, különböző végpontvédelmi megoldásokat (kötelező VPN használat a vállalat saját hálózatán kívül), illetve akár egy esetleges gyanús e-mail vagy telefonhívás kapcsán bárki felkeresheti az illetékes incidenskezelő csoportot. Habár az igazán kifinomult adathalász támadások pontosan ezeket az intézkedéseket kerülik ki észrevétlenül, hiszen pszichológiai manipulációt és mindenki számára elérhető nyílt információkat felhasználva férkőznek olyan munkavállalók közelébe, akik egy esetleges gyanús tartalmú e-mailt nem ismernek fel, és megteszik, amit a levélben írnak, ha az épp elég meggyőző és neki szól.

Az audit során kiküldött adathalász e-mailt az információbiztonsági csapat készítette, majd felügyelte az esetleges visszajelzéseket is. Például, ha valaki bejelentette, hogy gyanús levelet kapott, választ kellett visszaküldeni, melyben elmagyaráztuk, hogy ez csak egy általunk kreált adathalász levél, de köszönjük, hogy jelezte.

A szimuláció célja

Az általunk megalkotott adathalász e-mail egy adathalász kampány részét képezte. Ez a kampány részben az októberi kiberbiztonsági hónap előzetes felmérése miatt jött létre, részben pedig a közelgő belső audit miatt. Évente négyszer tartunk általában ehhez hasonló belső adathalász kampányokat (lokálisan) és másik négy alkalommal anyavállalati szinten kerülnek kiküldésre ilyen e-mailek. Ezek száma változhat például nagyobb globális adatszivárgások esetén, mivel ilyenkor felfrissítjük a munkatársaink biztonságtudatosságát, vagy esetleges magasabb linkre kattintási arányt eredményező kampány esetén (mely meghaladja a 10%-ot) újabbal készülünk a biztonságtudatosság fenntartása érdekében.

Minden biztonságtudatosságot célzó kampány legfontosabb mozzanata a cél megnevezése. Ez azért nagyon fontos, mivel a célkitűzésnek illeszkednie kell a vállalat saját biztonságtudatossági stratégiájához. Ezt időnként módosítják, felülvizsgálják, illetve bővítik, így más és más időszakokban végzett kampányok célkitűzései ezek szerint változnak.

Az adott adathalász kampányt megelőző kampányok mindig fontos szerepet játszanak az újabb tervezésében. Amennyiben egy adathalász kampány eredménye (lokális vagy vállalati csoport szinten) eléri a 10%-os kattintási arányt további tudatossági akciókat szerveznek (cikkek megjelentetése a belső intranet hálózaton, egyéni tudatosítási előadásokat szerveznek, vagy akár megkeresik a rosszabbul teljesítő vállalati területeket és direkt képzést nyújtanak).

Az adathalász e-mailünk jelenlegi célja kisebb részben volt a kiberbiztonsági hónap. Nagyobb részben a cél nem volt más, mint a közelgő belső auditra való felkészülés. Egy belső audit során a legfontosabb, hogy a vállalat tisztában legyen a saját, és a követelményeknek való megfeleléseivel (vagy épp a nem megfelelőségekkel), valamint lehetséges

jövőbeli fejlesztésekkel. A hasonló kampányoknál évente meghatározzuk, hogy milyen biztonságtudatosítási tevékenységeket végzünk (például adathalász kampányok száma, oktatások száma és témája, októberi „kiberhónap" eseményei).

Az általunk vizsgált esetben kampányunk célját akkor érjük el, amint megkapjuk a végleges adatokat arról, hogy a kiküldött e-mailek közül hány esetben lett volna éles helyzetben sikeres a támadásunk. Mivel ez megmutatja, hányan nem ismerik, illetve nem tartják be a vállalat információbiztonsági szabályzatát.

Az adathalász kampány

A teszt lefolytatásához a vállalat által ilyen esetekben használt Lucy Security szoftvert használtuk. A svájci Lucy Security egy kiberbiztonsági tudatosság fejlesztő szoftver. A kiberbiztonsági tudatosságot növelő tréning innovációi lehetővé teszik a szervezetek számára, hogy mérjék, javítsák és teszteljék alkalmazottaik biztonság-tudatosságát. Több támadássablon és sok testre szabható, képzési modul közül választhatunk. Első lépésként egy új kampányt, azon belül pedig egy új forgatókönyvet hoztunk létre. Mikor ezzel elkészültünk, különböző előre gyártott sablonok közül válogathattunk, de akár kreálhattunk is egy saját tematikájú kampányt. Fontos szempont volt, hogy az általunk használt sablon rendelkezzen magyar nyelvű „landing page-dzsel", és üzenettel. A mi esetünkben egy Google értesítés alapú kampányt választottunk, hiszen a vállalatnál fontos szabály, hogy a Google egyik szolgáltatását sem használják a kollégák, adatvédelmi szempontok miatt. Így az első intő jel lehetett az olvasóknak az, hogy Google-fiók értesítőt kaptak a céges e-mail címükre. Az általunk kiküldött üzenet az 1. ábrán látható:


Google

Kedves Google felhasználó!

Google-fiókjának helyreállítási telefonszáma nemrég megváltozott. Ha végrehajtotta ezt a módosítást, akkor nem kell többet tennie.

Ha nem Ön változtatta meg helyreállítási telefonszámát, előfordulhat, hogy valaki feltörte a fiókját. További információért látogassa meg ezt a linket: https://support.google.com/accounts/bin/answer.py?answer=2450236.

Ha problémái vannak a fiókjához való hozzáféréssel, állítsa vissza jelszavát az alábbi gombra kattintva:

Jelszó törlése

Üdvözlettel,
The Google Support csapat

This email can't receive replies. For more information, visit the Google Accounts Help Center.

You received this mandatory email service announcement to update you about important changes to your Google product or account

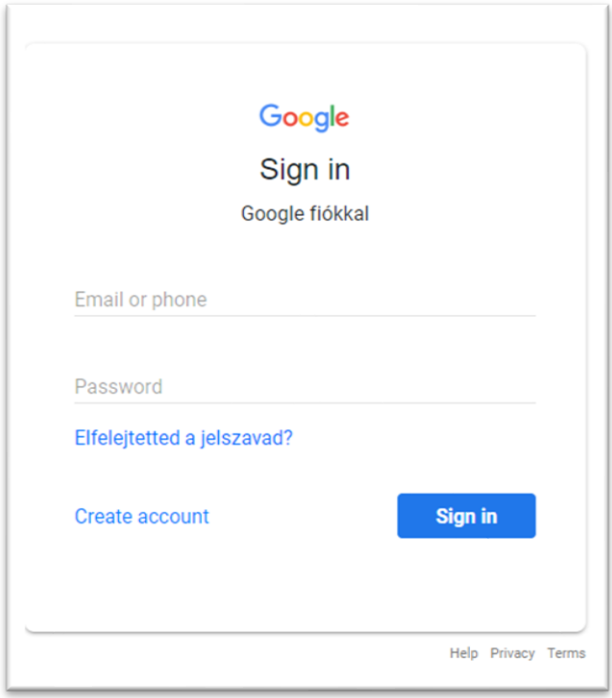
©2018, Google Inc., 160 Amphitheatre Parkway, Mountain View, CA 94043, USA

Please note that the third-party logos and trademarks used in this email or landing page are used for illustrative or instructional purposes only and there is no connection or relationship between the trademark owner and Lucy Security or the LUCY Security customer.

1. ábra A kiküldött üzenet (saját szerkesztés)

Az e-mail feladójaként egy általunk kreált e-mailcím jelent meg, mely goggle.sup@cloudserver185.com volt. A tárgymezőben pedig „Valaki feltörhette a Google fiókodat” szerepelt. Azok a kollégák, akik figyelmesen elolvasták a feladó e-mail címét, már a levél megnyitása előtt rájöhettek, hogy gyanús e-mail érkezett a postafiókjukba, hiszen a Google-re nem jellemző e-mailcím a feladó. A szöveg tartalmi része a mi esetünkben különösen testhezállónak bizonyult, mivel a vállalatnál nemrégiben telefonszolgáltató váltás történt, így a figyelmetlenebb kollégák könnyen összekapcsolhatták a SIM kártyák cseréjét ezzel az üzenettel.

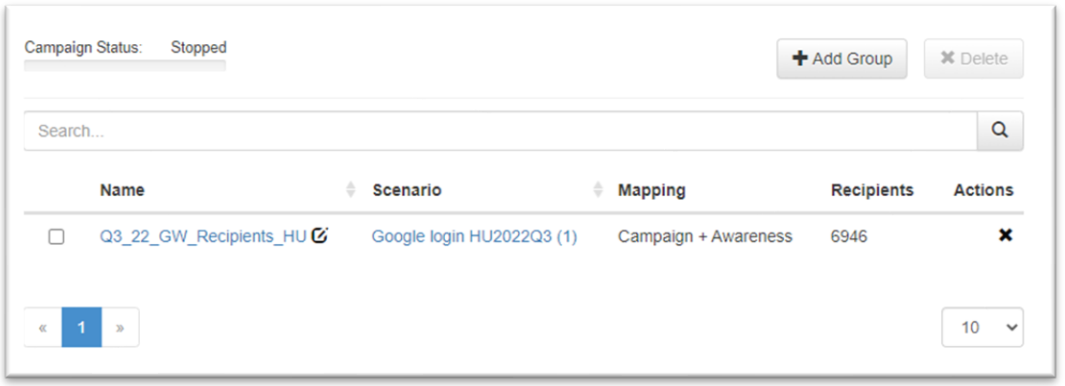
Azonban, ha valaki végig olvasta az apróbetűs részt is az üzenet alján, egyértelműen látszik, hogy a Lucy Security program által generált adathalász szimulációról van szó. Abban az esetben, ha a megadott linkre kattintottak, egy új böngészőoldal nyílt meg, mely a 2. ábrán látható.



2. ábra Az oldal, melyre a link vezetett (saját szerkesztés)

A képen jól látszik, hogy a felugró bejelentkező ablak félig magyarul, félig angolul van, ami szintén gyanús lehetett a kollégáknak.

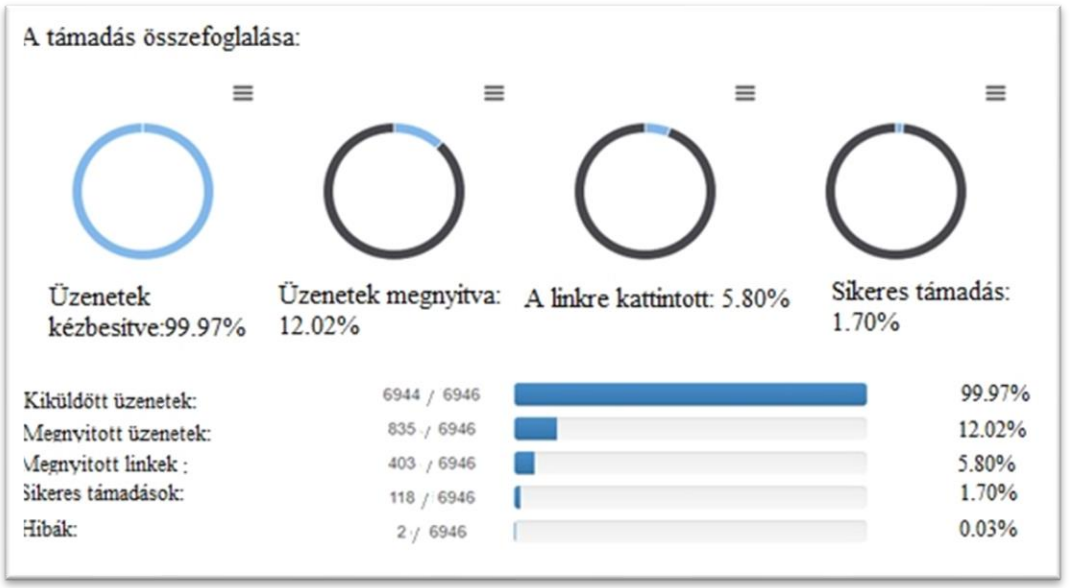
Miután elkészültünk az ál e-maillel, megadtuk a kampánnyal tesztelni kívánt dolgozók csoportját. A mi esetünkben ez a vállalat összes magyarországi dolgozóját magában foglalta. A 3. ábrán azt a felhasználói csoportot mutatjuk be, mely a vállalat által kiadott összes e-mail címet tartalmazza. (A felső vezetőktől a gyakornokokig) Ahogy az a 3. ábrán is látszik, végül az e-mail 6946 címre került kiküldésre.



3. ábra A vállalati csoport kiválasztása (saját szerkesztés)

Az eredmények

Az adathalász kampányunk nagyjából egy hétig tartott. Az e-mailek kiküldését követő két napban volt észlelhető a legtöbb linkre kattintás és sikeres támadás. Ezt követően a számuk drasztikusan csökkent. Végül a szoftver által egy hét múlva megkaptuk az adathalász szimuláció eredményét, melyet a 4. ábra mutat be:



4. ábra A támadási szimuláció eredményei (saját szerkesztés)

Jól látszik, hogy a kiküldött 6946db e-mail közül 6944 db sikeresen kézbesítve lett. A két meghiúsult kézbesítés valószínűleg épp a kilépés folyamatában levő kollégát, vagy már nem létező e-mailcímet jelöl. A levelet megkapó kollégák alig több mint 12%-a nyitotta meg a levelet, így elmondható, hogy szerencsére a dolgozók többsége tisztában van vele, hogy a vállalat semmilyen formában nem használja a Google szolgáltatásait. Még kevesebb,

a megnyitók csupán 5.8%-a kattintott a linkre, melyből 1.7% volt sikeres támadásnak tekinthető, azaz a kollégák megadták személyes adataikat.

Az általunk az előbbiekben referált szabályzat a vállalat saját információbiztonsági szabályzata. Épp ezért konkrétumok nélkül térhetünk csak ki rá. A szabályzat először meghatározza saját hatókörét és a fogalmakat és rövidítéseket melyek a dokumentumban szerepelnek. Ezután ismerteti a munkavállalók felelősségét, mely egyértelműen kijelenti, hogy minden munkavállaló az általa kezelt információk biztonságáért felel és felelősségre vonható. Az információk biztonsági besorolásának ismertetése fontos része a szabályzatnak. Ez alapján lehet: nyilvános, belső, bizalmas vagy szigorúan bizalmas egy adat. A besorolás alapján részletesen leírja az adott információk kezelésére vonatkozó előírásokat. A minősített adatok fogalmának és kezelésének szerves részét képezi a 2009. évi CLV törvény a minősített adat védelméről; valamint a GDPR adatvédelme és megfelelései. Ezek után a szabályzat ismerteti a jelszóhasználati szabályokat, hogy a lehető legbiztonságosabb, nehezen feltörhető jelszavakkal legyenek biztosítva a céges felhasználói fiókok.

A következő részben pedig az általunk előbbiekben említett szabályt ismerteti, miszerint a vállalat eszközeire csak és kizárólag a vállalat által jóváhagyott szoftverek és fájlok telepíthetőek vagy tölthetőek le. A vállalat által kiadott IT eszközök kizárólag üzleti célokra használhatóak egészen addig amíg a munkavállaló vezetője máshogy nem rendelkezik. (Egy ilyen döntésbe azonban kötelező a hozzáértő IT-s személyzet véleményét kikérni.)

A szabályzat a továbbiakban ismerteti:

- a biztonságos internet használatot,
- a biztonsági mentések fontosságát,
- a „tiszta asztal” elvet,
- az információ biztonságos megosztására vonatkozó szabályokat (például titkosított e-mailek)
- az információkezelést, információs rendszer fejlesztést és bevezetést
- a külső állományra, szolgáltatókra és partnerekre vonatkozó biztonsági előírásokat
- a naplózásra, jelentésekre és ellenőrzésekre vonatkozó előírásokat
- a gyanús viselkedés, biztonsági incidensek jelentését és az ehhez szükséges kapcsolattartási elérhetőségeket

Ezek után az utolsó részben bemutat egy rövid kockázat elemzést, a szabályozott tevékenységek felügyeletét, és ismerteti a szabályzatra vonatkozó hivatkozásokat és kapcsolatokat.

Mivel az általunk kapott a számadatok a 10%-os vállalat által meghatározott linkre kattintási határ alatt vannak, így annyiban tér el az eredmény a megszokottól, hogy nem volt szükség plusz tudatossági akciókat bevezetni. Úgy döntöttünk elég egy cikket írnunk róla, a munkatársak tájékoztatásának érdekében. Amennyiben az eredmény meghaladta volna a 10%-t, egyéni tudatosítási előadásokat szerveztünk volna, vagy megkerestük volna a roszszabbul teljesítő területeket és területre szabott képzést nyújtottunk volna nekik.

JAVASLATOK AZ INFORMÁCIÓBIZTONSÁG-TUDATOSSÁG FEJLESZTÉSÉRE

Egy nagyvállalati rendszerben a biztonság mindig kulcsfontosságú kérdés. Mind fizikai mind információbiztonsági oldalról. A következőkben az utóbbi témát mutatjuk be,

pontosabban azt, hogy milyen eszközökkel lehet és érdemes az információbiztonság-tudatosságot fejleszteni egy nagyvállalati környezetben.

Információbiztonság-tudatosság fejlesztése és javaslatok

Minden vállalat (vagy vállalkozás) életében nagy szerepet kap a munkavállalók felkészítése az esetleges webes fenyegetésekre, adat- vagy információlopásokra. De a vállalat növekedésével (és minél fontosabb pozíciójával) könnyen célkeresztbe kerülhet. Gyakrabban lehet kitéve social engineering támadásoknak, hacker támadásoknak, és egyéb fenyegetettségeknek, melyek célja az információszerzés, a vállalat hírnevének rombolása, vagy akár a teljes megsemmisítés.

Ezek miatt kap hatalmas szerepet és figyelmet az információbiztonság-tudatossági oktatás. Mivel a legkönnyebben kihasználható információbiztonsági rés maga az ember, mint tényező, a támadók bármilyen eszközt bevethetnek, hogy megszerezzék amire szükségük van. A rendszeres információbiztonsági oktatásokkal azonban a munkatársakban rejlő kockázat csökkenthető. Minél többször találkoznak valós támadásokhoz hasonló helyzetekkel, annál felkészültebben éri őket egy igazi élesben zajló támadás. Az információbiztonság-tudatossági tréning sikerét nagyban befolyásolja az oktatás minősége és a módszerek. A munkatársak az alábbi alapvető elvárásokkal kell megismerniük a tréning során:

- Tiszta asztal elv alkalmazása
- Tiszta képernyő használata
- Kulcsok, kártyák rendeltetésszerű kezelése
- Hardver eszközök és adathordozók kezelése, valamint tárolása
- A jelszavakkal kapcsolatos előírások betartása
- Iratmegsemmisítés helyes elvégzése
- Adathalász-gyanús e-mailek és egyéb technikák felismerése
- Vírusvédelem megfelelő alkalmazása
- Közösségi média használata (a vállalt területén és a magánéletben)
- Okos eszközök rendeltetésszerű, biztonságos használata
- Egyéb az adott vállalatra érvényes szabályok [8][9][10]

A tiszta asztal és tiszta képernyő: Az iroda kialakításakor arra kell törekedni, hogy a dolgozók és más esetlegesen a szobában tartózkodó személyek minél kevésbé lássanak rá a monitorokra. Az íróasztalon nem szabad látható helyen érzékeny adattal bíró dokumentumokat, feljegyzéseket tárolni. Ugyan így tilos a jelszavakat kiragasztani az asztal környékén, az irodában és bárhol, ahol illetéktelen személyek felhasználhatnák. Ugyan így nem tanácsos naplóban vagy kis könyvben tartani sem. Inkább használjuk valamely jelszókezelő programot melyhez a hozzáférést a vállalat biztosítja. A munkaidő lejártával az ehhez hasonló dokumentumokat elzárt helyen kell tartani. Mikor elhagyjuk a munkaállomást, a számítógépet lezárt (mai Windows operációs rendszereknél például a Windows-gomb és „L” együttes lenyomásával) vagy kikapcsolt állapotban kell az irodában hagyni. Ekkor külön figyelmet kell fordítani arra is, hogy a fénymásológépekben, nyomtatókban ne hagyjunk érzékeny iratot. Ha valamilyen okból kifolyólag vendég van az irodában, semmi esetre se hagyjuk egyedül, hiszen alkalma nyílhat kutakodni a dokumentumok között, illetve a fiókokban, szekrényekben. Az utolsó munkatárs, aki a nap folyamán elhagyja az irodát, ha van lehetősége, kulccsal zárja az irodát.

Kulcsok, kártyák rendeltetésszerű kezelése: A kulcsok és belépőkártyák kizárólag illetékes személyeknek adhatók ki. Amennyiben vendég érkezik az irodába, például egy megbeszélés miatt, érdemes megkérni a kollégát, akihez jött, hogy együtt közlekedjenek a látogatás idején az épületben. A kulcsok vagy kártyák kiadásáról, visszavételéről, esetleges cseréjéről vagy bevonásáról és megsemmisítéséről minden esetben nyilvántartást kell vezetni, mely a lehető legnaprakészebb állapotban kell legyen. Fontos, hogy a munkavállalók ismerjék a kulcsok és belépőkártyák használatának szabályait (például, hogy nem adhatják oda vagy nem adhatják kölcsön senki másnak stb.). A szabályok ismertetése, ha elmarad, komoly következményei lehetnek.

Hardver eszközök és adathordozók kezelése, valamint tárolása: A munkatársaknak kiemelt fontosságú megismernie a különböző hardverek és adathordozók helyes használatát. Ezek egyik első és talán legfontosabb szabálya, hogy ha a vállalat nem a „hozd a saját eszközöd" alapján működik, akkor saját adathordozót nem csatlakoztathat senki a vállalat hálózatán működő gépekre. Ez a szabály ugyan úgy vonatkozik okostelefonokra, táblagépekre és egyéb okos eszközökre is.

A jelszavakkal kapcsolatos előírások betartása: Sok esetben a vállalatok saját elvárásokat támasztanak a munkavállalókkal szemben arra vonatkozóan, hogy milyen jelszavakat kell bizonyos felületen használniuk. A könnyebb megjegyezhetőség és a maximális biztonság érdekében, a legtöbb cég ma már saját jelszókezelő szoftvert ad a dolgozók kezébe, így a hosszabb, biztonságosabb jelszavakat nem szükséges megjegyezni, sem pedig papírcetlikre írva kiragasztani valahova. Fontos tudatosítani a kollégákban, hogy a jelszavakat ne osszák meg se egymással, se senkivel. Egymás belépési kulcsait pedig szintén ne használják és ne engedjék másnak sem, hogy így tegyenek.

Iratmegsemmisítés helyes elvégzése: Egy cég életében mindig keletkeznek olyan dokumentumok, melyekre már esetleg nincs is szükség, azonban még mindig tartalmazhatnak olyan adatokat, melyek illetéktelen személy kezébe kerülve kárt okozhatnának. Ezeket mindig a megfelelő körültekintéssel kell tárolni s megsemmisíteni. Fontos tudatosítani a kollégákban, hogy ilyen esetben nem csak papírlapokra kell gondolni. lehetek ezek borítékok, belépőkártyák, külső adathordozók is. Az iratmegsemmisítés mindig olyan mértékű kell legyen, hogy az adott tárgy helyreállítása többe kerüljön (akár időben akár pénzben) mint az általa hordozott információ értéke.

Adathalász-gyanús e-mailek és egyéb technikák felismerése: A munkatársak érzékenyítése az ilyen szituációkra nagyon fontos. Akár egy egész vállalat sorsa is múlhat egy adathalász támadáson. Ezért lényeges, hogy a gyanús e-maileket és egyéb kétes megkereséseket (mobiltelefonos hívás, SMS, személyes beszélgetéssel stb.) gyorsan felismerjék, valamint tudják, hogy hol kell bejelenteniük. Ez minden vállalatnál más lehet, de biztosan az információbiztonsági osztályhoz van köze.

Vírusvédelem megfelelő alkalmazása: A munkatársak gyakran értesítést kapnak a legújabb frissítésekről, melyeket a számítógépen eszközölniük kell. Ezt semmiképp sem szabad elmulasztaniuk, hiszen az IT részleg kifejezetten azért küldi ezeket az értesítéseket,

hogy a vállalat összes használatban lévő eszközét friss, naprakész szoftverrel használjuk. Ezzel igyekeznek csökkenteni az esetleges sérülékenységekből adódó támadások kialakulásának esélyeit.

Közösségi média használata: Napjainkban szinte már nincs olyan személy, aki valamilyen formában nem lenne jelen a közösségi médiában. Sajnos emiatt a legtöbben tudtukon kívül is áldozatául eshetnek egy támadónak, aki épp kiválasztja ki legyen az áldozata a következő social engineering támadás során. Ezért fontos a munkavállalókban tudatosítani, hogy mit lehet és mit nem lehet közzétenni a közösségi média oldalakon.

Íme néhány példa:

- ne osszuk meg a helyzetünket
- ne tegyünk közzé képet melyek az irodában vagy a vállalat telephelyein belül készülnek
- ne osszunk meg belső vállalati adatokat
- ne osszunk meg a jelszavakra utaló képeket, szövegeket
- semmiképp se osszuk meg a lakcímet, telefonszámot, és egyéb olyan személyes adatokat melyekkel esetleg valaki visszaélhet
- ne adjunk ki anyagi helyzetünkre utaló képeket, videókat

Abban az esetben, ha egy munkavállaló mégis megoszt a fentiekhez hasonló tartalmakat, veszélybe sodorhatja a vállalatot. Ezért fontos, a helyes oktatás és az ott hallott információk elsajátítása. Pont a fent említett okok miatt egyes vállalatok megtiltják a közösségi média oldalak látogatását a saját hálózatukról.

Okos eszközök rendeltetésszerű, biztonságos használata: A közösségi média mellett, az okos eszközök használata szintén népszerű manapság. Azonban fontos a munkavállalók tudtára adni hogyan lehet egy adott vállalati környezetben használni őket. Amennyiben saját, és nem céges eszközről van szó, még nagyobb odafigyelésre van szükség. Többek között fontos ismertetni a kollégákkal, hogy hol és mikor lehet az eszközöket telefonálásra, video hívásra, vagy akár fényképezésre használni. Ez vállalatonként változhat, annak függvényében, hogy milyen pozícióban dolgozik az illető, és mivel foglalkozik maga a cég. Az ilyen eszközök töltése is fontos, hogy említést tegyünk róla, mivel akár vírussal fertőzöttek is lehetnek. Így semmiképp sem javasolt a vállalati hálózathoz csatlakoztatott céges eszközökről tölteni őket. Ugyan ezen okból kifolyólag fontos az is, hogy nem csak a vállalat által kiadott laptopokra és asztali gépekre, de a céges okoseszközökre sem javasolt ismeretlen vagy nem megbízható forrásból származó applikációkat letölteni. (Például játékokat és más alkalmazásokat a Play Áruházból vagy az Appstore-ról.)

Egyéb az adott vállalatra érvényes szabályok: Minden vállalat maga írja elő a fent említett pontokkal szemben támasztott elvárásait. Ezek nagyban függenek a cég profiljától, és attól, hogy pontosan mivel is foglalkoznak. Ez azért fontos, mert a különböző ágazatokban más és más fenyegetettségek fordulhatnak elő. Ilyenek lehetnek például a know-how adatbázis védelme egy gyár esetében, vagy akár egy energiaszolgáltató vállalat komplex védelme, mely energiával látja el az egész országot.

A fentiek ismeretében már megfogalmazható egy a vállaltra szabott információbiztonság-tudatossági oktatás. Azonban az oktatás sikere nem csak a belső tartalmától függ, hanem az oktatás természetétől is. Ahhoz, hogy a legmegfelelőbbet válasszuk, ismernünk kell a lehetőségeinket, melyek a következők:

- Hagyományos, személyes oktatás
- E-learning kurzus
- Online oktatás (Microsoft Teams, Zoom stb.)
- Kampány
- Szabadulószoba
- Társasjáték

A **hagyományos, személyes oktatás** pozitívuma lehet, hogy van kapcsolat a résztvevők és az oktató közt. Azonban hátránya, hogy egy klasszikus frontális tanteremi (vagy tárgyalói) helyzet nem ösztönzi a munkatársakat az interakcióra. Ezáltal unalmassá válhat az oktatás, és így a résztvevők kevésbé figyelnek oda, sajátítják el a leadott anyag lényegét. Ez azért számít nagy hátránynak, mivel az információbiztonság-tudatossági tréningek egyik leglényegesebb része, hogy a megfelelő gondolkodásmódot sajátítsák el a munkavállalók, mellyel könnyebben eldönthetik, hogy az adott helyzetben szükséges-e támadásra gyanakodniuk.

Az **e-learning kurzus és az online oktatás** sok szempontból hasonlít egymásra. Pozitívumai, hogy nem szükséges a fizikai részvétel, így akár home officeból, vagy a pandémia miatt a megfelelő távolságtartással is elvégezhetőek ezek a kurzusok. Az e-learning kurzusok jó megoldást jelentenek akkor, ha csak általános ismétlő jellegű figyelemfelhívásra van szükség a munkatársak körében. Azonban hátránya lehet, hogy ezeket gyakran nem a kellő odafigyeléssel végzik el a kollégák, így az eredménye ilyen esetben ugyan az lehet, mint a személyes oktatásnak. Az online oktatásra is ugyan ez vonatkozik, azonban itt még az is nehezítheti a kollégák koncentrációját, hogy ha egy olyan előadáson vesznek részt, melyben nincs szükség arra, hogy kérdésekre válaszoljanak, interakcióba lépjenek egymással, könnyen elterelődik a figyelmük. Ez főleg abban az esetben igaz, ha home office-ból csatlakoznak be a hívásba.

A **biztonságtudatossági kampányok** célja, hogy az információbiztonság-tudatosság teljesen beépüljön a vállalati kultúrába. Ez azt jelenti, hogy minden alkalmazott automatikusan figyelembe veszi a biztonsági szempontokat minden döntésében és minden, a vállalat érdekében tett intézkedésében. Ahhoz, hogy ezt elérjék, az információbiztonságnak mindennapos témává kell válnia, amely gyakran foglalkoztatja a kollégákat. A kampányok egyszerre több csatornán is futtathatóak, így a leghatásosabb, ha a vállalat által használt belső „hírportálon" és a valóságban is minden nap találkoznak ezzel a témával a munkavállalók. Hátránya az, hogy nem fenntartható állandóan a figyelem, amit erre tudnak fordítani a munkavállalók. Például megszokják a kiplakátolt figyelemfelhívásokat és nem olvassák el őket egy idő után.

Abban, hogy a munkavállalók érdeklődését egy oktatás alatt fenntartsuk, sokat segíthet a **gamifikáció**. A gamifikáció, azaz „játékosítás" a játékszerű ösztönző elemek beépítését jelenti a mindennapi vagy nem játék jellegű tevékenységekbe. Bármikor, amikor játékszerű funkciókat vagy a játéktervezés szempontjait alkalmazzák nem játék jellegű kontextusban, játékosítás történik. Így nem csak élvezhető, de könnyebben tanulható is az elsajátításra szánt tananyag. Oroszi Eszter munkája során sokszor alkalmazza a gamifikációt különböző információbiztonság-tudatossági oktatások keretein belül. Erre példa lehet a szabadulószoba és a társasjáték. Ezekkel a technikákkal játékosan, unalom és „felesleges ismétlés" (mivel sajnos sok kolléga így tekint a kötelezően ismétlődő oktatásokra) nélkül a gyakorlatban tanulják meg és alkalmazzák a munkatársak az információbiztonsági szabályokat. A szabadulószoba és a társasjáték hatékony tud lenni, hiszen leköti és elgondolkodtatja a munkatársakat. Azonban hátránya lehet például, hogy a személyes oktatáshoz hasonlóan kevésbé rugalmas megoldás szervezési szempontból, valamint lehetséges, hogy ebben a formában nem lehet minden témát olyan alapossággal ismertetni, mint például egy jól megszervezett kampánysorozattal, vagy esetleg egy személyes oktatás során.

ÖSSZEFOGLALÁS

Tanulmányunkban bemutattuk, hogy mi az audit és milyen fontos a helyes auditálás, valamint az, hogy milyen nagy szerepe van az információbiztonsági auditoknak egy vállalat sikerében és biztonságában. Említést tettünk arról, milyen tulajdonságokkal rendelkezik egy jó auditor, és választ adtunk a kérdésre miért fontos, hogy a social engineering technikák részét képezzék az információbiztonsági auditoknak. A téma empirikus vizsgálatát egy esettanulmány segítségével és a kapott eredmények elemzésével végeztük el. A lezajlott adathalász kampány és a kutatás eredményeként, írásművünk végén ismertettük az információbiztonság-tudatosság fejlesztési eszközeit majd egy rövid javaslatot tettünk arra vonatkozóan, hogy mivel lehet még hatékonyabbá tenni a munkatársak oktatását az információbiztonsági-tudatossági tréningeken.

FELHASZNÁLT IRODALOM

[1] Molnár B. – Kő A. *Információrendszerek auditálása. Az informatika és az információrendszerek ellenőrzési és irányítási módszerei*. Budapest: Corvinno Technology Transfer Kft. 2009.
[2] Horváth Zs. L. *Információbiztonsági belső auditor* (jegyzet), 2016. megtekintve: 2022.07.28
[3] Ködmön I. *Hétpecsétes történetek: Információbiztonság az ISO 27001 tükrében*, 2008. megtekintve: 2022.09.15
[4] Kerti A. *Az audit tevékenységek előkészítése*, (belső oktatási anyag). megtekintve: 2022.05.25
[5] Baglyos S. *Az információbiztonsági auditálás fontossága* (https://www.ludovika.hu/blogok/cyberblog/2022/06/23/az-informaciobiztonsagi-auditalas-fontossaga). megtekintve: 2022.10.16
[6] Oroszi E. *Információbiztonsági stratégia és vezetés*. Budapest: Nemzeti Közszolgálati Egyetem. 2014.

[7] Michelberger P. – Lábodi Cs: *Vállalati információbiztonság szervezése*. Budapest: Óbudai Egyetem. 2012.
[8] Oroszi E. *Időutazás a Social Engineering auditok korában, avagy mi változott az elmúlt 10 év alatt?* (https://silentsignal.hu/docs/S2_ISACA_Konferencia_Oroszi_Eszter_20220616.pdf). megtekintve: 2022.10.12
[9] Oroszi E. *Biztonságtudatossági játékok, avagy a felhasználók információbiztonsági ismereteit fejlesztő módszerek hatékonyságának vizsgálata* (https://silentsignal.hu/docs/S2_ISACA_masodik_szerda_OE_20220112.pdf). megtekintve: 2022.10.12
[10] Oroszi E. – Bálint B: *Biztonságtudatossági szabaduló szoba, avagy a felhasználók biztonságtudatosságának új fejlesztési eszköze* (https://www.witsec.hu/sites/default/files/WITSEC2019/4_3_witsec_szabadulo_prezi_20191010.pdf). megtekintve: 2022.10.12
[11] Kollár Cs. *Hackerpszichológia*. Az Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar „Kutatók éjszakája 2017" rendezvényen elhangzott előadás prezentációja. https://www.slideshare.net/drkollarcsaba/hackerpszichologia. megtekintve: 2022.10.15.

FELHASZNÁLT SZABVÁNYOK

[12] MSZ ISO/IEC 27001:2014