HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

FELSŐVEZETŐI BIZTONSÁGTUDATOSÍTÁS SZEREPE

MAGYAR SÁNDOR

EIVOK

HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

KIHÍVÁSOK

- Felsővezetők általában nem IT előképzettséggel rendelkeznek, hanem például jogász vagy közgazdász végzettséggel. Nem minden esetben érzékenyek a téma iránt, nem értik az informatikai, információbiztonsági szakma terminológiáját.
- Előfordul, hogy túlzott bizalom van a technológia iránt vagy pont annak az ellentéte, a kételkedés van túlsúlyban.
- Feltörekvő, felforgató technológiák fejlődnek (pl.: MI, kvantum számítástechnika stb.).
- Social engineering technikák fejlődnek.
- A nyílt forrású információszerzés (OSINT) lehetőségei az internet penetrációjával egyre jobban megnövekedtek.
- Az álhírek terjedése, hatása növekszik.

HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

MIELŐTT EZEK A MONDATOK ELHANGOZNÁNAK…

- Ez egy jó program rakjátok fel azonnal!
- Nekem rendszergazdai jogosultság kell!
- Rám ne legyen érvényes ez a bonyolult jelszószabály!
- El akarom érni a rendszert otthonról is!
- Eddig sem történt semmi!
- A mi adatainkra senki sem kíváncsi!
- Ne vegyük ki a munkavállalókat feleslegesen a munkából!
- Ennek az egyhetes tanfolyam árából egy felsőfokú végzettséget is meg lehetne szerezni, nem kell!
- Elegen vagytok már!

eivok
HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

MIÉRT KELL TUDATOSÍTANI A FELSŐVEZETŐKET?

- Amíg nem érkezett, érkezik támadás a kibertérből, addig felesleges kiadásnak tűnhet a drága informatikai rendszerek hardver és szoftver elemeit, amelyeknek az éves karbantartási és licensz díjai is jelentősek.
- Hiábavaló költségként lehet értelmezni a szervezetnél a megfelelő számú és képzettségű IT, IT biztonsági szakember alkalmazását, a szervezet méretétől függően biztonsági műveleti központok üzemeltetését stb.
- Továbbá az információbiztonsági tudatosítás is szükségtelen erőforrás pazarlásnak tűnhet.
- …

eivok
HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

FELHASZNÁLÓK	FELSŐVEZETŐK
• Hozzáférés néhány rendszerhez • Korlátozott jogosultságok a rendszerekhez • Érzékeny információk az e-mail fiókokban • A felhasználók kevesebb mappát láthatnak • Kevesebb befolyás • Alacsonyabb reputációs kockázat	• Több rendszerhez való hozzáférés lehetősége • Magasabb szintű jogosultságok a rendszerekhez • Több érzékeny információ az e-mail fiókokban • A felsővezetők több mappát láthatnak • Nagyobb befolyás • Nagyobb célpont • Nagyobb a reputrációs kockázat

HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

FONTOS SZEMPONTOK

- Az információbiztonsági tudatosítást nem lehet uniformizáltan kezelni.
- A felsővezetők részéről elkövetett hibák a szervezet reputációs kockázatát is növelik, mivel sok esetben azonosítják a szervezetet, vagy a szervezeti egységet a vezető személyével.
- A vezetői tudatosítás nagy részben kis csoportos, esetleg egyéni végrehajtást igényel, mivel a vezetőkre nagyobb figyelmet kell szánni és a tudatosítás során feltett kérdéseiket is mindenképpen meg kell válaszolni, módosítva ezzel az esetleges tematikát.
- A vezetői leterheltség miatt az információbiztonsági tudatosítás időpontjait és ütemezését külön előre egyeztetés során kell megállapítani.

VEZETŐI TUDATOSÍTÁSNÁL FIGYELEMBE KELL VENNI

- Egyéni jellemzők is befolyásolják a tudatosítás végrehajtását, amit figyelembe szükséges venni. Többek között az életkor és az azzal járó generációs különbségek, az iskolai, szakmai végzettség, a szervezeti hierarchiában betöltött pozíció, korábbi információbiztonsági események átélése is befolyással lehet a tudatosítás végrehajtása során.

KIBERVÉDELMI GYAKORLATOK SZEREPE A VEZETŐI TUDATOSÍTÁS ESETÉBEN

- Az életben a sikeres kibertámadás elszenvedése után előfordulhat, hogy a vezetőknek olyan szituációkban kell megfelelő döntést hozni, vagy esetleg nyilatkozni, amelyek számukra nem teljesen megszokott. Az esemény súlyosságának függvényében akár a felsővezető szint azonnali döntései, válságkommunikációja válik szükségessé.
- A kibervédelmi gyakorlatok során meg lehet érteni, hogy ha az informatikai állomány létszáma és képzettsége nem megfelelő, abban az esetben milyen szintű támadásokat lehet elszenvedni. További meg lehet ismerni, hogy mi a következménye a hardening hiányának, milyen detektáló technológiák alkalmazása szükséges, mi a log fájlok gyűjtésének, elemzésének feladata, hogyan lehet reagálni megfelelően egy incidensre, hogyan lehet hatékony munkafolyamatokat építeni stb.

ÖSSZEGZÉS

- Amennyiben az üzleti folyamatok vannak kizárólag szem előtt tartva és nem jut elég erőforrás a védelmi intézkedésekre, abban az esetben a kibertámadások sikeressége nagyobb lesz a szervezetnél.
- A felsővezetők esetében a stratégiai gondolkodás megvan, azonban a kibertér és abból érkező fenyegetésekre történő reagálás nem minden esetben. Az információbiztonsági tudatosítás eredménye lehet a stratégiákba beépített kiberbiztonsági terület erősítése.

FELHASZNÁLT IRODALOM

- Dobák I. (2019), OSINT - Gondolatok a kérdéskörhöz, Nemzetbiztonsági Szemle 2019/2, pp. 83-93.
- Legárd, Ildikó (2021), Játék a jövőért: Az információbiztonsági tudatosság fejlesztési lehetősége egy gamifikált applikáció segítségével, POLGÁRI SZEMLE: GAZDASÁGI ÉS TÁRSADALMI FOLYÓIRAT 17 : 1-3 pp. 358-373., 16 p. (2021)
- Kő Andrea, Tarján Gábor, Mitev Ariel (2023), Information security awareness maturity: conceptual and practical aspects in Hungarian organizations, INFORMATION TECHNOLOGY AND PEOPLE 36 : 8 pp. 174-195., 22 p. (2023)
- Maeyer, D.D. (2007). Setting up an effective information security awareness programme. In ISSE/SECURE 2007 Securing Electronic Business Processes (pp. 49-58).
- Olt, Christian; Gerlach, Jin; Sonnenschein, Rabea; and Buxmann, Peter (2019), "On the Benefits of Senior Executives' Information Security Awareness" (2019). ICIS 2019 Proceedings. 25.
- https://aisel.aisnet.org/icis2019/cyber_security_privacy_ethics_IS/cyber_security_privacy/25
- SANS Top Ten Security Awareness Topics – Roundup, https://www.sans.org/blog/top-ten-security-awareness-topics-roundup/
- Sonnenschein, Rabea; Loske, André; and Buxmann, Peter, "The Role of Top Managers' IT Security Awareness in Organizational IT Security Management" (2017). ICIS 2017 Proceedings. 13. https://aisel.aisnet.org/icis2017/Security/Presentations/13
- Tarján (2023): Az információbiztonsági tudatosság érettségi szintjének mérése szervezetekben, Doktori Értekezés, Budapesti Corvinus Egyetem, 2020.
- Verizon 2023 Data Breach Investigations Report (DBIR) https://www.verizon.com/business/resources/reports/dbir/
- Vikman László: Az aktuális kibertér fenyegetés jogi kihívástérképe, Katonai Jogi és Hadijogi Szemle 2022/3., 91-108.

eivok
HÍRKÖZLÉSI ÉS INFORMATIKAI
TUDOMÁNYOS EGYESÜLET
INFORMÁCIÓBIZTONSÁGI
SZAKOSZTÁLY

KÖSZÖNÖM SZÉPEN A MEGTISZTELŐ FIGYELMET!