A BETEGEK RÁNK BÍZZÁK AZ ÉLETÜKET, DE MI VAJON MEGFELELŐEN VÉDJÜK ŐKET A KIBERVESZÉLYEKTŐL?

Az alábbiakban bemutatjuk az egészségügyi ágazatot fenyegető **öt legfontosabb kiberbiztonsági fenyegetést** és tippeket adunk azok enyhítésére!

K1berh0nap@2023 OKTÓBER

E-MAIL ADATHALÁSZAT (PHISHING)

Az e-mailes adathalászat arra irányuló kísérlet, hogy e-mailt használva rávegyenek arra, hogy személyes adatokat adjunk meg, vagy olyan fertőzött linkekre kattintsunk, amelyek révén a hackerek hozzáférhetnek a betegeink összes adatához.

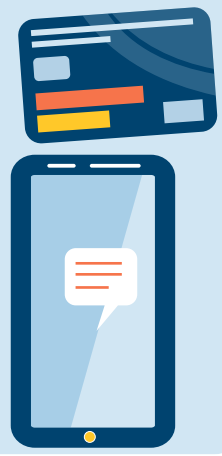
A sikeres támadások 90%-a ilyen adathalászattal indul!

- A fájlok csapdák lehetnek! Ellenőrizze azokat, mielőtt a beágyazott hivatkozásokra kattint!
- A weboldalak csalók is lehetnek; saját maga írja be az URL-eket, és ne linken keresztül érje el azokat!
- A jelszóval védett dokumentumok csalások is lehetnek; kinyitás előtt ellenőrizze azokat!

ESZKÖZÖK ELVESZTÉSE VAGY ELLOPÁSA

Tudta? A mindennapi eszközök, például laptopok, okostelefonok és USB-meghajtók gyakran elvesznek vagy ellopják, és idegenek kezébe kerülhetnek.

- Soha ne hagyja felügyelet nélkül laptopját vagy berendezését!
- Mindig titkosítsa az érzékeny adatokat, amelyek a készülékein vannak!
- Azonnal értesítse az informatikust, vagy a kijelölt személyt, ha az eszköze elvész!



ZSAROLÓVÍRUS TÁMADÁSOK (RANSOMWARE)

Ransomware támadás egy olyan hackertámadás esetén valósul meg, amikor az adatok titkosításával megszerzik az adatainkat, vagy a számítógépes rendszereink feletti felügyeletet mindaddig, amíg nem fizetünk váltságdíjat. Ez veszélybe sodorhatja a betegek ellátását, és megakadályozza Önt és a kórházat abban, hogy időben gondoskodjon a betegekről!

- A legtöbb zsarolóvírus támadás e-mail adathalászattal indul, ezért vegye figyelembe az ott leírt óvintézkedéseket!
- Tartsa be az adatmentés szervezeti szabályait, illetve a 3-2-1-es szabályt, és egy változat mindig legyen offline!

BENNFENTES, VÉLETLEN, ILLETVE SZÁNDÉKOS ADATVESZTÉS

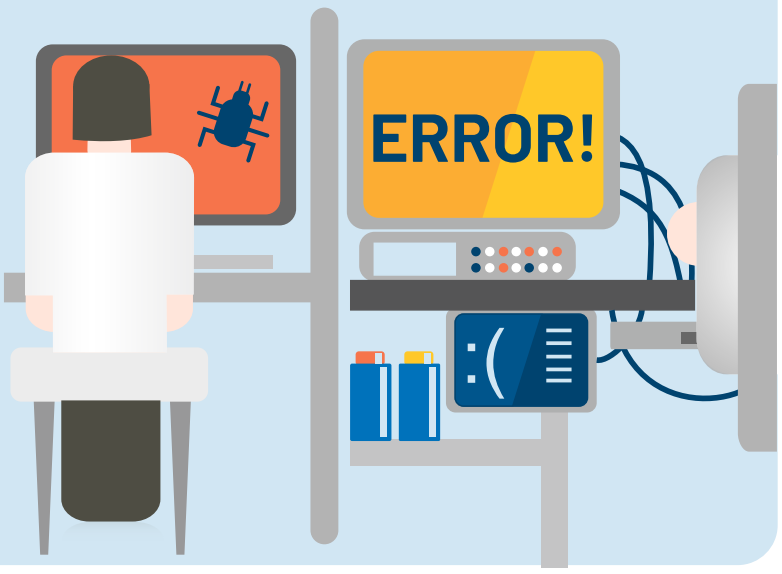
Bennfentes fenyegetések minden szervezetben léteznek, ahol alkalmazottak, vállalkozók vagy más felhasználók hozzáférnek a szervezet technológiai infrastruktúrájához, hálózatához vagy adatbázisaihoz.

- Hallgasson az ösztöneire, és mindig jelezze azt, ha valami szokatlan, nem megfelelő történik a betegadatokkal vagy az informatikai rendszerrel!
- Véletlen tévedések folytán is előfordulnak adatvesztések vagy adatkezelési problémák (pl.: e-mail cím elgépelése). Ha ilyen történik, azonnal értesítse a kijelölt szakembert, hogy megfelelően be lehessen avatkozni a további problémák megelőzése érdekében!
- Védje meg a betegek adatait azáltal is, hogy nem ad ki információkat, kivéve, ha megfelelően azonosította a kérelmező személyazonosságát!

TÁMADÁSOK A CSATLAKOZTATOTT ORVOSI ESZKÖZÖK ELLEN

Vegyük fontolóra a következőket: a kórház egy adathalász támadás áldozata, amely révén több kardiológiai monitorhoz csatlakoztatott szerver is érintetté válik. A támadás a rendszer teljes irányítását teszi lehetővé a hacker számára, így tetszés szerint ki- és bekapcsolhatja a rendszereket!

- A kórház védelme érdekében tájékozódjon, hogy hogyan lehet használni az informatikai rendszerhez kapcsolódó orvosi és nem orvosi eszközöket!
- A leggyakoribb problémát a lejárt támogatású vagy régi eszközök jelentik, ezért minden esetben tájékozódjon, hogy ezek alkalmasak-e az informatikai rendszerhez történő csatlakozásra és megfelelően frissített szoftverrel rendelkeznek-e!



Tájékozódjon a friss egészségügyi kiberbiztonsági hírekről!

MEMT Magyar Egészségügyi Menedzsment Társaság

Semmelweis Egyetem EMK Egészségügyi Menedzserképző Központ

SZTFH

1996 Nemzetbiztonsági Szakszolgálat

NEMZETI KIBERVÉDELMI INTÉZET