KIBERFENYEGETÉSEK AZ EGÉSZSÉGÜGYBEN

Valamilyen szinten minden egészségügyi intézmény fenyegetett.
A fenyegetés érkezhet kívülről vagy belülről, lehet rosszindulatú vagy akár véletlen is.
Ezeknek a fenyegetéseknek a szervezetre gyakorolt hatása attól függ, hogy a fenyegetés képes-e kihasználni a meglevő sebezhetőségeket.
Az egészségügyi adatok védelme érdekében elengedhetetlen, hogy tisztában legyen azokkal a veszélyekkel, amelyek hatással lehetnek a betegellátásra!

FENYEGETÉS

ZSAROLÓVÍRUS (RANSOMWARE) TÁMADÁS

A zsarolóvírusok olyan rosszindulatú programok (malware), amelyek jellemzője, hogy megkísérlik megakadályozni a felhasználói adatokhoz a hozzáférést: az adatokat olyan kulccsal titkosítják, amelyet csak a támadó ismer, és csak váltságdíj ellenében adja át a megtámadottnak.

SZOLGÁLTATÁSMEGTAGADÁSI TÁMADÁS

Miután egy vírus megfertőzte a hálózatot, a támadó szolgáltatásmegtagadási támadást hajthat végre, amely teljesen elérhetetlenné teszi a hálózat erőforrásait. Ez hatással lehet a betegellátásra, és megzavarhatja a hálózatok, az orvosi alkalmazások és eszközök működését.

VÍRUSTÁMADÁS

Amint egy vírus bejutott a rendszerbe, az káros lehet a teljes hálózatra és rendszerre nézve, mert megrongálja azokat vagy megsemmisíti az értékes egészségügyi adatokat.

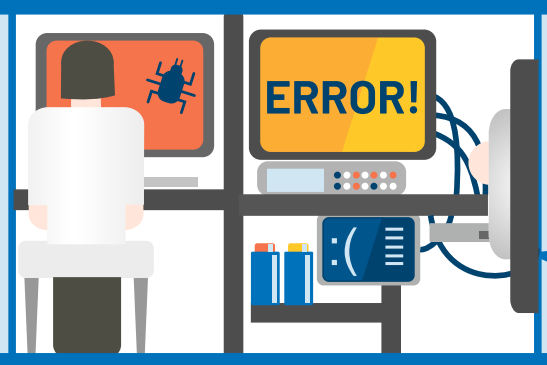
BRUTE FORCE ATTACK

A támadó brute force támadást alkalmazhat a hozzáféréshez úgy, hogy algoritmus segítségével mindaddig próbálkozik a jelszavak karaktereinek kombinációjával, amíg egyezést nem talál.
Ez lehetővé teszi számukra, hogy belépjenek a hálózatokba és alkalmazásokba, ahol az értékes egészségügyi adatokat tárolják.

PSZICHOLÓGIAI MANIPULÁCIÓ

Sok támadás az emberi gyengeségek kihasználására alapul: pl. egy rosszindulatú linket tartalmazó adathalász e-maillel vagy sms-el kezdődik, és ha rákattint, az komoly kiberbiztonsági kockázatokat jelenthet a hálózatra és a szervezetre nézve.

EGÉSZSÉGÜGYI INTÉZMÉNY



MEGOLDÁS

Szervezeti szinten szükséges koordinálni és megoldani,hogy megfelelő végpont-védelem legyen!
Az alapvető spam és antivírus megoldásokat telepíteni szükséges és naprakészen frissen kell tartani!

A hálózati forgalom folyamatos figyelése szükséges. Ahol jelentős növekedést lát, ott szolgáltatásmegtagadási támadás lehetősége merülhet fel.
Ebben az esetben a végpont karanténba helyezése váhat szükségessé, amely megelőzheti illetve csökkentheti a károkat.

A szervezetnek központilag kell biztosítania, hogy az alapvető spam/ antivírus szoftverek telepítve és aktíválva legyenek és automatikusan frissüljenek.
Ahol csak lehetséges, észlelést követően távolítsák el a jogosulatlan szoftver-alkalmazásokat!

Korlátozni szükséges a hitelesítési próbálkozások számát és időbeliségét!
Az időkorlát alapvetően megakadályozza azt a lehetőséget, hogy "nyers erővel" kikényszerítsék a j elszót!

A többtényezős hitelesítést (MFA) kell minél szélesebb körben alkalmazni.
Az MFA egy nagyon hatásos módszer a támadók azon képességének korlátozására, hogy kompromittálja a szervezet informatikai környezetét.

Az infografika a https://405d.hhs.gov/ szakmai anyagai alapján készült.

Tájékozódjon a friss egészségügyi kiberbiztonsági hírekről!

MEMT Magyar Egészségügyi Menedzsment Társaság

Semmelweis Egyetem EMK Egészségügyi Menedzserképző Központ

SZTFH

1996 Nemzetbiztonsági Szakszolgálat

NEMZETI KIBERVÉDELMI INTÉZET