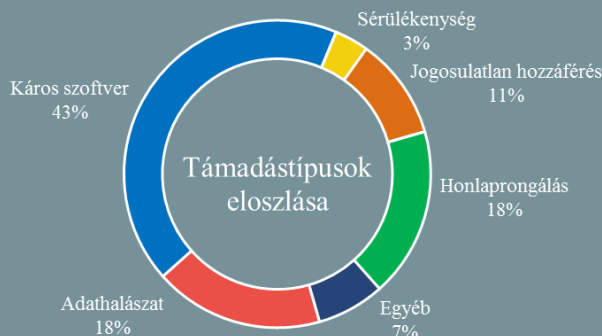


Az NKI által kezelt incidensekre vonatkozó statisztikai adatok:  
2020.06.19. - 2020.06.25.



Kövessen minket megújult [weboldalunkon](#), ahol friss IT-biztonsági hírek kerülnek publikálásra!

## Megkerülő megoldás az Outlook indításakor tapasztalható hibára

(bleepingcomputer.com)

A Microsoft [közlése szerint](#) azon felhasználók, akik frissítettek az **Outlook 2005 Build 12827.20268** vagy ennél frissebb verziójára, a program indításakor hibát tapasztalhatnak. A hibaüzenet (“Something is wrong with one of your data files and Outlook needs to close. Outlook might be able to fix your file. Click OK to run the Inbox Repair Tool.”) ugyan az Inbox Repair Tool futtatását irányozza elő, azonban a felhasználók hiába kattintják végig az abban szereplő lépéseket, az nem oldja meg a problémát. **Bővebben...**

## EU: zéró tolerancia lép életbe a kórházak elleni kibertámadásokkal szemben

(ec.europa.eu)

Ursula von der Leyen, az Európai Bizottság elnöke sajtóközleményben számolt be a 2020. június 22-ei EU-Kína csúcstalálkozó eredményéről. Az EU a tárgyalat témakörök kapcsán kifejezetten határozott véleményt fogalmazott meg, többek között a kórházak és más adatközpontok elleni kibertámadások, valamint az online dezinformáció terjesztésének elítéléséről.

## Egy új malware adatlopó trójaivá változtatja a Discord klienst

(bleepingcomputer.com)

A MalwareHunterTeam által felfedezett NitroHack nevű káros kód magát egy szoftver cracknek álcázza, ami látszólag szabad hozzáférést ad a Discord Nitro-hoz, a Discord prémium szolgáltatásához, azonban telepítéskor a káros kód módosítja a Windowsos Discord klienst, ami ezután már egy szenzitív adatok ellopását lehetővé tévő trójaiként fog működni. A malware hitelesítő adatok és pénzügyi információk után kutat, majd direkt üzenetek útján megpróbál továbbterjedni az áldozat ismerősei között. A felhasználók úgy ellenőrizhetik, hogy érintettek-e a fertőzésben, hogy Jegyzetomb (NotePad) segítségével megnyitják a `%AppData%\Discord\0.0.306\modules\discord_voice\index.js` fájlt, és ellenőrzik a fájl végét, ami ha nem került módosításra, a `module.exports = VoiceEngine;` bejegyzéssel végződik. **Bővebben...**

## Exchange szerverek elleni web shell malware támadásokra figyelmeztet a Microsoft

(securityaffairs.co)

Exchange levelezőszerverek elleni támadásokra [figyelmeztet](#) a Microsoft, védekezési javaslatokat is közzétéve. Két fő technikáról számolnak be: a leggyakoribb forgatókönyv szerint a támadók adathalászat, vagy káros kódokat tartalmazó weboldalak segítségével támadják a végpontokat hitelesítő adatok megszerzését célozva, majd a hálózaton továbbterjedve jutnak el az Exchange szerverig. **Bővebben...**

## Linuxon és Androidon is elérhető a Microsoft Defender Advanced Threat Protection

(bleepingcomputer.com)

Microsoft Defender Advanced Threat Protection (ATP) védelmi szolgáltatása immáron Linuxon és Androidon is elérhető, utóbbi esetében azonban még csupán nyilvános béta állapotban. A linuxos verzió jelenleg a RHEL 7.2+, CentOS Linux 7.2+, Ubuntu 16 LTS, SLES 12+, Debian 9+, Oracle Linux 7.2. disztribúciókon telepíthető, amihez rendelkezni kell érvényes Microsoft Defender ATP for Servers licenccel. A program telepítése és konfigurálása Puppet, Ansible, vagy bármilyen más konfigurációkezelő eszközzel lehetséges, erről bővebb információ [innen](#) érhető el. **Bővebben...**

## IT biztonsági Tanács



Az NBSZ NKI [weboldalán](#) hasznos információkat olvashat a a PISAX platformról.