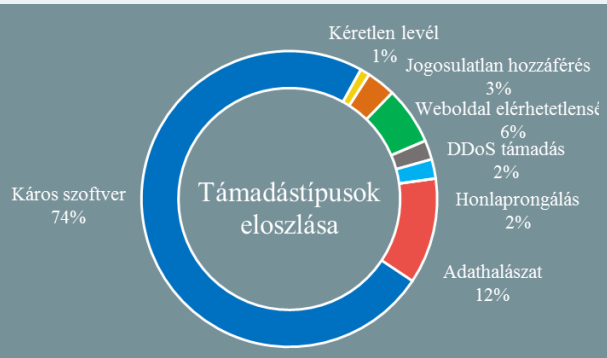
Nemzetközi IT-biztonsági sajtószemle

2020. 14. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2020.03.27. - 2020.04.02.



Kövessen minket megújult weboldalunkon, ahol friss IT-biztonsági hírek kerülnek publikálásra!

Szlovákia: a parlament jóváhagyta az állami hozzáférést a mobiltelefon-adatokhoz

(heise.de)

Szlovákia állami egészségügyi hatósága a jövőben hozzáférhet az állampolgárok mobiltelefon-adataihoz. A szlovák parlament gyorsított eljárásban fogadta el a törvénymódosítást, amely lehetővé teszi az állam számára az állampolgárok egyébként védett mobiltelefon adatainak elérését. Ez azt jelenti, hogy az állami egészségügyi hatóság a mobiltelefon helymeghatározási adatait felhasználhatja annak nyomon követésére, hogy az új koronavírussal fertőzött polgárok hol tartózkodnak és kivel találkoznak. **Bővebben...**

Adatvédelmi aggályokat vet fel a Kínában bevezetett egészségügyi alkalmazás

(theguardian.com)

Kínában több – főleg a COVID-19 járvány miatt lezárt tartományban – bevezetésre került egy "egészségkód" nevű rendszer, amely nagymértékben befolyásolja az állampolgárok szabad mozgását. Mindezt telefonos alkalmazások segítségével üzemeltetik, amelyek városonként és tartományonként némileg eltérőek lehetnek, azonban működésük alapja azonos. A kínai polgárokat – egészségügyi állapotuk, valamint utazási előzményeik alapján – egy színkóddal látják el. **Bővebben...**

IT biztonsági Tanács

Az NBSZ NKI weboldalán hasznos információkat olvashat arra vonatkozóan, hogy mire érdemes figyelni a gyermekek videójátékozásával kapcsolatban karantén idején.

Komoly fenyegetésként értékeli a NATO a Kína által javasolt új internet architektúráját

(infosecurity-magazine.com)

A kínai kormányzat a jelenlegi TCP/IP protokollra épülő internetes architektúra megreformálásár tett javaslatát először tavaly szeptemberben nyújtotta be a Nemzetközi Távközlési Egyesületnek (ITU). A "New IP" névre keresztelt elképzelés arra hivatkozik, hogy a TCP/IP mára elavultá vált, számos sérülékenységtől szenved, és nem képes kiszolgálni az új technológiák (például az IoT, az űrbéli és holografikus kommunikáció) által támasztott igényeket. A megoldást a felterjesztés szerint egy "univerzális és jobban protokollált" rendszer jelentheti. **Bővebben...**

Windows login adatokat szivárogtat a Zoom kliens

(bleepingcomputer.com)

A windowsos Zoom kliens chat felülete UNC path injection támadások kivitelezésére ad lehetőséget. A sérülékenység oka, hogy chat üzenetek között bármilyen posztolt URL – így az UNC hálózati útvonala is – hiperlinké konvertálódik. Mindez azt jelenti, ha egy felhasználó egy ilyen linkre kattint, a Windows az SMB fájlmegosztási protokollt felhasználva megkísérli elérni a távoli erőforrást, amely a problémát felfedező biztonsági kutató demonstrációjában a cat.jpg nevű fájl. Ennek során a Windows alapértelmezésben elküldi a felhasználó bejelentkezési adatait, azaz a felhasználónevet, illetve a jelszó hash-t, amelyet a támadó így megszerezhet és feltörhet. **Bővebben...**

MS SQL szerverek veszélyben

(thehackernews.com)

Egy 2018 májusa óta tartó malware kampányra (Vollgar) hívják fel a figyelmet kiberbiztonsági kutatók, amelynek során a támadók káros kódokat telepítenek MS SQL szerverekre. A Guardicore Labs szerint a támadók az internet felől elérhető, gyenge jelszóval védett SQL szerverekre vadásznak, az elmúlt hetek során pedig rendkívül aktívak voltak, naponta 2-3 ezer adatbázis szervert fertőztek meg. A kutatók közreadtak egy szkriptet is, ami rendszer adminok számára nyújthat segítséget annak megállapításában hogy a felügyeletük alatt álló adatbázisokat érintettek-e. **Bővebben...**