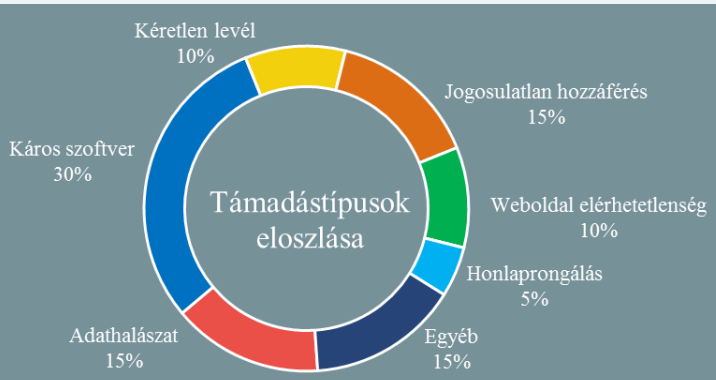
Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2019.10.04. - 2019.10.10.



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

E-mail fiókok elleni célzott támadásokra figyelmeztet a Microsoft

(blogs.microsoft.com)

A Microsoft blogján egy korábban ismeretlen, feltételezetten iráni állami támogatású APT csoportról (Phosphorus) ad hírt, amely augusztus és szeptember között több, mint 2 700 alkalommal próbált meg Microsoft fiókokba illetéktelenül belépni. A támadott fiókok közös nevezője, hogy az amerikai elnökválasztási kampányhoz kötődnek, jórészt jelenlegi és volt amerikai kormányzati tisztviselőkhöz, valamint politikai témákat feldolgozó újságírókhoz tartoztak. A Phosphorus csoport kiterjedt információgyűjtést végzett a célpontok tekintetében, majd ezeket felhasználva valamilyen módon jelszó visszaállítást igyekeztek kikényszeríteni az áldozattól. Az esetet felfedező Microsoft fenyegetés felderítő részlege (Microsoft Threat Intelligence Center – MSTIC) szerint a támadások technikai értelemben nem számítottak kifinomultnak, azonban a jelentős mennyiségű személyes információ felhasználása arra utal, hogy a csoport erősen motivált és komoly idő, valamint energiabefektetéssel végzi a tevékenységét. **Bővebben...**

A Thunderbird integrálja az e-mail titkosítást az OpenPGP szabvány használatával

(heise.de)

A jövőben a Thunderbird levelezőprogram képes lesz a közvetlen PGP titkosításra és dekódolásra, így a korábban használt EnigMail kiegészítő feleslegessé válik. Azoknak, akik korábban PGP-vel szerették volna titkosítani az e-mail-eket, egy kiegészítőt kellett telepíteniük, ami felelt a titkosításért, az aláírásért és a kulcskezelésért, ez pedig a Mozilla Thunderbird-ben az EnigMail volt. A 2020 nyarára tervezett Thunderbird 78 -tól azonban maga a nyílt forráskódú levelező látja majd el ezeket a funkciókat. **Bővebben...**

Amerikai segítséggel javítanák az energiaszektor kibervédelmét a balti térségben

(securityweek.com)

Megállapodás született arról, hogy az Amerikai Egyesült Államok segítséget nyújt a balti országoknak az energiahálózataik kibertámadásokkal szembeni ellenállóképességének növeléséhez. Habár Észtország, Lettország és Litvánia már 2004 óta tagjai az Európai Uniónak és az Észak-Atlanti szövetségnek, továbbra is az orosz energiaellátásra támaszkodnak, azonban ez komoly kitettséget jelent a Litvánia szerint folyamatos orosz kiberfenyegetéssel szemben. **Bővebben...**

Harmadik felek reklám célra használhatták Twitter felhasználók biztonsági célból megadott személyes adatait

(bleepingcomputer.com)

A Twitter közleménye szerint elképzelhető, hogy egy hiba miatt egyes felhasználók azon telefonszámai és e-mail címei, amelyeket biztonsági célból — a kétfaktoros hitelesítés miatt — adtak meg, reklámcéllal kerülhettek felhasználásra a közösségi oldal Tailored Audiences and Partner Audiences szolgáltatása révén. A Tailored Audiences arra ad lehetőséget a hirdetőknek, hogy egy — akár harmadik féltől származó — marketing lista feltöltésével célzott reklámot tudjanak küldeni ügyfeleik számára a telefonszámuk, vagy e-mail címük alapján. A Twitter közleménye szerint jelenleg nincs pontos képük arról, hogy a szeptember 17-én felfedezett probléma pontosan hány felhasználót érinthetett, azonban mindent megtesznek azért, hogy az eset ne ismétlődhessen meg.

Az egyiptomi kormány mobil malware-ekkel kémkedik aktivisták és a politikai ellenzék után

(securityaffairs.co)

Az egyiptomi kormány kifinomult módszerekkel kémkedik állampolgárai után, figyelmeztet a Check Point jelentése. A megfigyelési program célszemélyei között elsősorban újságírók, aktivisták, politikusok és jogászok szerepeltek. A Check Point azután kezdett vizsgálódni az ügyben, miután az Amnesty International márciusban nyilvánosságra hozta az újságírók és emberi jogi képviselők ellen folytatott támadásokról szóló jelentését. A kémkedési műveletek mobilalkalmazásokon keresztül kerültek végrehajtásra, amelyek közül néhány a Google Play Store alkalmazásboltból is elérhető volt, ilyen például a Gmail kiegészítő Secure Mail, az iLoud200% tárhely kezelő applikáció és az IndexY. A rosszindulatú alkalmazások segítségével a támadók képesek voltak megkerülni a biztonsági beállításokat, így hozzáférhettek az e-mail fiókok bejelentkezési adataihoz, valamint a hívásnaplókhoz. **Bővebben...**

IT biztonsági Tanács

A technológia számos kényelmi funkciót biztosíthat, azt azonban fontos tudni, hogy az internethez kapcsolódó okoseszközök (IoT) komoly biztonsági kockázatot jelenthetnek. Akkor járunk el helyesen, ha egy-egy ilyen eszköz megvásárlásakor figyelembe vesszük, hogy ezzel egyúttal támadási felületet is nyújtunk illetéktelenek számára, hogy hozzáférjenek személyes adatainkhoz – mint a tartózkodási helyünk, egészségügyi állapotunk – vagy például IP kamerákon keresztül személyes életterünkhöz. Az NBSZ NKI weboldalán javaslatokat talál arra vonatkozóan, hogy mit érdemes szem előtt tartani egy IoT berendezés megvásárlása előtt.

Új botnet fenyegeti a windowsos rendszereket

(eackingnews.com)

A Guardicore Labs biztonsági cég szerint a Smominru botnet közel 47 000 PC-t fertőz meg naponta, ezzel egyike a legnagyobb arányban fertőző botneteknek jelenleg. A támadás során a – néhány évvel ezelőtt a WannaCry zsarolóvírus terjesztésére is használt – NSA-féle EternalBlue exploit-ot alkalmazza, valamint gyengén védett RDP, Telnet és MS-SQL fiókok után kutat. A jelentés szerint eddig a legtöbb támadás az Amerikai Egyesült Államokban, Oroszországban, Kínában, Tajvanon és Brazíliában történt, ezek mintegy 85%-ában Windows 7, valamint Windows Server 2008 rendszerek álltak a célkeresztben.

Az EU ebben látja az 5G hálózatok főbb kockázatait

(eu2019.fi)

Megjelent a NIS Együttműködési Csoport által elkészített, uniós szintű jelentés az 5G hálózatok biztonságára vonatkozóan. Az EU-s tagállamok összehangolt kockázatelemzése során előállt anyag egyértelműsíti, hogy a nagyobb funkcionalitás több veszélyt hordoz magában. Mivel az 5G hálózatok nagyobb mértékben hagyatkoznak majd a szoftverekre, a támadóknak is kiterjedtebb lehetőségük lesz káros kódok, például backdoorok alkalmazására. Komoly kockázatot jelent, hogy a hálózatok üzemeltetői a korábbi technológiákhoz képest sokkal inkább támaszkodnak majd a szállítókra, ami nem csupán a támadási felületet, de a támadások potenciális hatását is növeli. Ennek kapcsán különös fontossággal bír az egyes szállítók kockázati profilja, amelynek megalkotásakor azt is figyelembe kell venni, hogy az adott cégen keresztül potenciálisan mekkora befolyást képes gyakorolni egy nem EU-s állam. **Bővebben...**

Egyszerűsödik a bűnügyi adatok megosztása az Egyesült Királyság és az Amerikai Egyesült Államok között

(infosecurity-magazine.com)

Bűnügyi adatok megosztására vonatkozó kétoldalú brit-amerikai megállapodás született, amelynek értelmében mind az USA, mind az Egyesült Királyság bűnüldöző hatóságai egyszerűbben és gyorsabban szerezhetnek majd be bűncselekményekkel összefüggő elektronikus adatokat a másik országban működő szolgáltatóktól. Jelenleg a rendvédelmi szerveknek 6 hónaptól két évig is eltarthat, mire hozzáférnek a kérvényezett információkhoz, az új elképzelés szerint azonban ez mindössze hét napra csökkenne. A várakozások szerint elsősorban egyirányú lesz az adatáramlás, és főleg az amerikai tech cégek fognak adatot szolgáltatni az Egyesült Királyságbeli cégek számára. Több szervezet is üdvözölte a hírt, egyesek azonban kockázatosnak vélik az időkeret szűkösségét, és attól tartanak ez jogosulatlan adatmegosztásokhoz vezethet.

A Samsung biztonságos Android változatot fejlesztett ki a Bundeswehr számára

(heise.de)

A Samsung az Android egy biztonságos változatán dolgozik a német hadsereg (Bundeswehr) és a német szövetségi rendőrség (Bundespolizei) számára. A Bundeswehr katonáinak a jövőben képesnek kell lenniük az okostelefonok szolgálati célokra történő széles körű felhasználására. Ennek érdekében a Samsung a dél-német Blackned informatikai és tanácsadó céggel együtt fejleszti az Android okostelefon operációs rendszerének speciális verzióját. Az új, Androidon alapuló, rendkívül biztonságos operációs rendszer kifejlesztésekor a Samsung Knox biztonsági szoftverét fogják alapul venni. **Bővebben...**