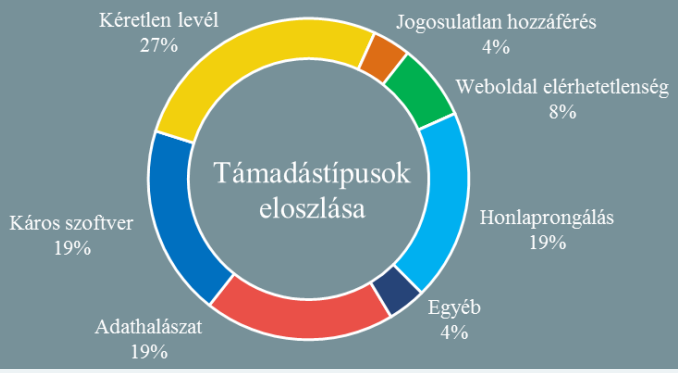
NEMZETI KIBERVÉDELMI INTÉZET

Nemzetközi IT-biztonsági sajtószemle

2019. 33. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2019.08.09. - 2019.08.15.



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

Ukrajna Észtország példáját követve bevezeti az elektronikus választásokat

(ehackingnews.com)

Az ukrán elnök Vladimir Zelensky csapata ígéretet tett arra, hogy a következő ─ 2024-ben esedékes ─ ukrán elnökválasztást az észt elektronikus technológiával kapcsolatos tapasztalatok felhasználásával rendezik meg, azaz az állampolgárok már elektronikusan is szavazhatnak majd. Jelenleg a világon csupán Észtország használ online rendszert a parlamenti választások lebonyolítására. A szavazók egy chip-azonosító kártya vagy mobile ID segítségével és egy PIN kóddal azonosíthatják magukat a rendszerbe való belépés során. Az ukrán hatóságok ezeket a lehetőségeket ki szeretnék bővíteni e-aláírással, mobil azonosítóval és esetlegesen egy telefonos Smart ID-val. A tervek szerint lehetőség lesz a szavazat módosítására is, valamint annak ellenőrzésére, hogy azt megfelelően vették-e figyelembe a szavazatszámláláskor. **Bővebben...**

Nem biztonságos módon kezeli az utasadatokat a British Airways

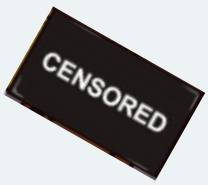
(securityweek.com)

Komoly kritika érte a British Airways (BA) légitársaságot, amiért egy, az elektronikus jegyfoglalási rendszerét érintő sérülékenység veszélyezteti az utasok adatainak biztonságát. A probléma nem szoftveres sérülékenység, hanem egy tervezési hiba eredménye, ami az ügyfeleknek e-mailekben kiküldött ellenőrző linkeket érinti. Ezek az URL-ek úgy kerültek kialakításra, hogy az utasoknak elég legyen rákattintaniuk a linkre, hogy megtekinthessék a foglalási adataikat. A biztonsági kockázat abban rejlik az URL-be ágyazott információk nem kerülnek titkosításra, ami azt jelenti, hogy egy illetéktelen személy az e-mailt megszerezve hozzáférést szerezhet az adott utas több személyazonosításra alkalmas (Personally Identifying Information – PII) adatához. **Bővebben...**

A Trump kormányzat cenzúrával lépne fel az állítólagos cenzúra ellen

(edition.cnn.com)

A CNN birtokába került egy elnöki rendelet vázlata („Protecting Americans from Online Censorship”), amely a Szövetségi Kommunikációs Bizottságot (Federal Communications Commission – FCC) arra utasítaná, hogy értelmezze újra, hogy a Communications Decency Act (CDA) hogyan és milyen esetben védi a közösségi média platformokat, amikor tartalmakat távolítanak el. Az 1996-os CDA 230-as szekciója jelen formájában éppen azt szavatolja, hogy az internetes cégek nem számon kérhetőek azon tartalmakért, amelyeket felhasználóik posztolnak, emellett széleskörű védelmet nyújt számukra a kifogásolható tartalmak eltávolításakor, amennyiben „jóhiszeműen” jártak el. **Bővebben...**



Személyiségtípusunk sérülékenyebbé tehet minket a kiberbűnözéssel szemben?

(darkreading.com)

Az ESET és a Myers-Briggs vállalat közös tanulmányban igyekezett felderíteni a személyiségvonások (traits) és a különböző kibertámadásokkal szembeni fogékonyság közötti összefüggéseket. Az emberi tényező szerepe a kibertámadások vonatkozásában igencsak jelentős. A Verizon idei adatszivárgásokat vizsgáló jelentésében azt találta, hogy a biztonsági események 20%-a vállalati dolgozóktól eredt, a Dtex ugyanakkor ennél lényegesebb szerepet tulajdonít a dolgozóknak, az ő felmérésük szerint az esetek kétharmadában (64%) lehet nekik tulajdonítani a problémát. **Bővebben...**

Szinte lehetetlen védekezni az androidos kártevők ellen

(techradar.com)

Bár a Google az elmúlt időszakban jelentős előrelépéseket tett annak érdekében, hogy a Play Store-ból eltávolításra kerüljenek a rosszindulatú alkalmazások, a Black Hat konferencia egy előadásán a Google Project Zero kutatója, Maddie Stone rávilágított arra, hogy rengeteg androidos eszköz előre telepített rosszindulatú alkalmazásokkal kerül forgalomba, amelyekkel szemben a felhasználóknak közel lehetetlen védekezniük. Jelenleg körülbelül 100 és 400 közé tehető az androidos eszközökre előre telepített alkalmazások száma, amelyek közül a kiberbűnözőknek elég egyetlen alkalmazást kompromittálniuk, hogy a teljes eszközt megfertőzzék. Stone, még az Android Security Team tagjaként több, az ellátási lánc során keletkező fertőzést azonosított, mint például a Chamois botnetet, amely 2016 óta ezidáig 21 millió eszközt érintett, amelyek közül mintegy 7,4 millió eszközön került előtelepítésre. **Bővebben...**

IT biztonsági Tanács

Online szolgáltatások igénybevétele során személyazonosságunk megerősítésének egyik lehetséges módja, ha videóhíváson keresztül, vagy egy fénykép készítésével bemutatjuk személyazonosításra alkalmas igazolványaink egyikét.

Az ilyen fényképek a számítógépes csalók számára többféle visszaélési módot tehetnek lehetővé, többek közt hamis online ─ például pénzmosásra alkalmas kriptovaluta váltó ─ fiókokat hozhatnak létre a nevünkben, amelynek eredményeként az elkövetők helyett nekünk kell majd szembenéznünk a jogi következményekkel.

Az NBSZ NKI weboldalán **itt** találja arra vonatkozóan javaslatainkat, hogy személyazonosító fényképeink ne kerülhessenek rossz kezekbe.

Úgy tűnik a GDPR-t is fel lehet használni adatlopáshoz

(nakedsecurity.sophos.com)

Az Oxford Egyetem egy PhD-s kutatója úgy találta, hogy túl sok cég ad ki úgy személyes adatot ügyfeleiről a GDPR által meghatározott „Hozzáférési jog” alapján benyújtott adatkérésekre válaszul, hogy az adatkérelmező személyét egyáltalán nem, vagy nem megfelelően ellenőrzi. James Pavur a menyasszonyát megszemélyesítve küldött adatkéréseket összesen 150 egyesült királyságbeli és amerikai vállalatnak. Az első 75 esetben csupán olyan adatokkal igazolta a személyazonosságot, amelyek online publikusan elérhetőek voltak, például a hölgy neve, e-mail címe, telefonszámai ─ amelyre válaszul egyes cégek kiadták a teljes lakcímét. **Bővebben...**

Új-Zéland elsőként legalizálja a bérek kriptovalutában történő kifizetését

(ehackingnews.com)

Új-Zéland adóhivatala, az Inland Revenue Department (IRD) engedélyezte, hogy a vállalatok digitális fizetőeszközökön fizethessék ki a béreket. Az erről szóló közleményt augusztus 7-én hozták nyilvánosságra, ebben arra hivatkoznak, hogy a döntést az 1994-es adóigazgatásról szóló törvény (Tax Administration Act) alapján hozták meg. Több megkötés is vonatkozik az új bérfizetési módra, a vállalatok például csak a hivatalos foglalkoztatási megállapodások alapján munkát vállaló alkalmazottak számára tudnak majd kriptovalutában fizetni, aminek közvetlenül átválthatónak kell lennie fiat valutára, valamint, hogy a kifizetés mértékét egy, vagy több fiat valutához igazítottan rögzíteniük kell. **Bővebben...**

Egy 20 éves Windows sérülékenységre derült fény

(zdnet.com)

A Google Project Zero Team egy ismert pentestere, Tavis Ormandy olyan windowsos sebezhetőséget azonosított, ami a Windows XP-től kezdődően minden verziót érint. A biztonsági hiba a Windows CTF protokolljában található, kihasználásával pedig illetéktelenek átvehetik az irányítást bármilyen alkalmazás, sőt az egész operációs rendszer felett. A CTF a Windows egy kevéssé dokumentált eleme, része a Text Services Frameworknek (TSF), amely a szövegek windowsos megjelenítését vezérli. Amikor a felhasználó elindít egy alkalmazást, a Windows ehhez egyúttal egy CTF klienst is létrehoz, ami a szervertől utasításokat fogad az operációs rendszer nyelvi beállításáról és a billentyűzet beviteli módjairól. **Bővebben...**

Több, mint 40 sérülékeny driver adhat módot jogosultság kiterjesztésre

(thehackernews.com)

A támadók számára egy kompromittált rendszer esetén kiemelten fontos a folyamatos hozzáférés biztosítása, amelynek elérése érdekében a különböző hardver elemeket érintő sérülékenységek gyakorta jutnak szerephez. Az egyik ilyen célcsoportot az illesztőprogramok (driverek) jelentik, ezek ugyanis, annak érdekében, hogy biztosíthassák a megfelelő kommunikációt egy hardver és az operációs rendszer között, jellemzően kernel módban, kiemelt jogosultsággal futnak. A most tárgyalt sérülékenység éppen emiatt veszélyes, mivel kihasználásával a támadó felhasználói jogosultsági szintről (Ring 3), kernel szintig (Ring 0) juthat, ezzel pedig képes lehet ─ többek közt ─ a felhasználó tudtán kívül backdoor-t telepíteni. **Bővebben...**