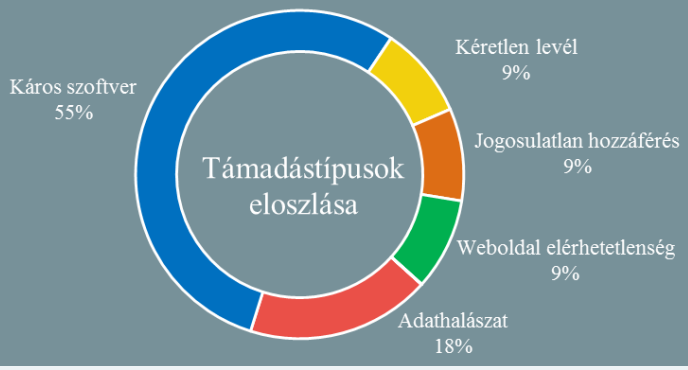
Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2019.10.18. - 2019.10.24.



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

A záró beszámoló szerint nem történt szándékos visszaélés Hillary Clinton e-mail botránya kapcsán

(heise.de)

Az USA külügyminisztériumának többéves vizsgálata – a volt amerikai külügyminiszter és elnökjelölt Hillary Clinton privát e-mail fiókjának hivatali célú használatával kapcsolatban – súlyosabb megállapítás nélkül ért véget. A nyomozás 2014-ben kezdődött, és a hatalmas médiafelhajtásnak köszönhetően, különösen a 2016-os elnöki kampány idején sokak figyelmét felkeltette. A záró jelentés kimondja, hogy bár a magánszerver hivatalos ügyekben történő használata növeli az illetéktelen hozzáférés kockázatát, „nincsenek meggyőző bizonyítékok a minősített információval történő szisztematikus, szándékos visszaélésére". A demokrata Hillary Clinton az Amerikai Egyesült Államok külügyminisztere volt 2009 és 2013 között, amely idő alatt magánszerveren keresztül folytatta kommunikációját anélkül, hogy erre engedélyt kapott volna. Az amerikai külügyminisztérium vizsgálatának a 2016-os kampány idején legjobban Clinton ellenfelei örülhettek. **Bővebben...**

Felszámoltak egy Csehországban működő orosz kémhálózatot

(securityaffairs.co)

A cseh rendőrség és a belföldi hírszerzés (BIS) felszámolt egy orosz kiberkémkedéssel foglalkozó hálózatot, amelynek pénzügyi támogatása a prágai orosz nagykövetségen keresztül zajlott. Michal Koudelka, a hírszerzés vezetőjének nyilatkozata szerint a leleplezett hálózat egy nagyobb szerveződés része volt, amelyet Oroszországból irányítanak és a műveleteit több, más európai ország területén is végzi. Augusztus során egy cseh parlamenti bizottság nyilvánosságra hozta a cseh kiberbiztonsági központjának (National Cyber and Information Security Agency) jelentését, ami egy külföldi hatalomnak tulajdonította az ország külügye elleni júniusi támadást.

Együttműködés a gyermekek online biztonságáért

(nki.gov.hu)

2019. október 22-én együttműködési megállapodást írt alá a Belügyminisztérium, a Nemzetközi Gyermekmentő Szolgálat Magyar Egyesület, valamint az Országos Rendőr-főkapitányság a gyermekek digitális térben történő fokozott védelméért. A megállapodás célja a kiskorúak fejlődésére káros tartalmak, valamint a gyermekek zaklatásának visszaszorítása és végső soron egy biztonságosabb kibertér megteremtése. Ennek részeként a szervezetek vállalták, hogy fokozott információ és adat megosztással segítik egymás munkáját, valamint tudástranszferrel szakmai ismereteik bővítését teszik lehetővé. **Bővebben...**

Adatszivárgás több VPN szolgáltatónál, titkosítási kulcsok kompromittálódtak

(securityaffairs.co)

Informatikai támadás érte a NordVPN, valamint a TorGuard VPN szolgáltatókat, ennek során ismeretlen hackerek elloptak és nyilvánosságra hoztak több privát titkosítási kulcsot, amelyek a cégek weboldalainak, valamint VPN konfigurációs fájljainak biztosítására szolgáltak. A támadás még tavaly történt, a támadók a NordVPN-t érintően legalább három privát kulcsot hoztak nyilvánosságra, a cég egy régebbi weboldal tanúsítványához tartozót ─ amely azóta lejárt ─, valamint két OpenVPN kulcsot. Szakértők attól tartanak, hogy a kulcsok publikálása lehetővé tehette, hogy illetéktelenek hamis VPN szervereket hozzanak létre, valamint hogy közbeékelődéses (Man-in-the-Middle) támadások során hozzáférjenek a felhasználók VPN forgalmához. **Bővebben...**

Közbeékelődéses támadást tesz lehetővé a UC Browser Androidon

(securityaffairs.co)

Több mint 600 millió UC Browser és UC Browser Mini Androidos felhasználó volt közbeékelődéses támadásnak (MitM) kitéve, köszönhetően annak, hogy a böngésző alkalmazás harmadik fél szerveréről, nem titkosított kapcsolaton keresztül tölt le egy APK (Android Package Kit) csomagot. A Zscaler biztonsági kutatói a böngésző kapcsán szokatlan hálózati kapcsolatra lettek figyelmesek a „9appsdownloading" domain irányába. A további vizsgálatok során kiderült, hogy az applikáció egy androidos csomagkészletet igyekszik letölteni, ráadásul nem biztonságos csatornán (HTTPS) keresztül, ami egyrészt megsérti a Google Play irányelveit, másrészt a nem biztonságos kapcsolat lehetővé teszi a felhasználók elleni közbeékelődéses támadások kivitelezését. Az APK elemzése során kiderült, hogy az a „9Apps" elnevezésű app-boltot takarja. A kutatók arra a problémára is rávilágítottak, hogy az APK külső tárba történő helyezése lehetőséget biztosít más alkalmazások számára, hogy a megfelelő jogosultságokkal módosíthassák az APK-t. **Bővebben...**

IT biztonsági Tanács

A technológiai fejlesztéseknek köszönhetően okoseszközeink igen hamar, akár egy-két év alatt is elavulttá válhatnak, hiszen a piacon folyamatosan jelennek meg a nagyobb teljesítményű készülékek, amelyek egyre több és több funkcióval bírnak.

Amennyiben szeretnénk megszabadulni a már elavult, vagy tönkrement eszközeinktől, fontos, hogy mindezt megfelelő módon tegyük, és tisztában legyünk annak lehetséges káros következményeivel. Az okoseszközök selejtezésére vonatkozó javaslatokat az NBSZ NKI weboldalán, itt találhat.

MSSQL 11 és 12 szerverek veszélyben

(securityweek.com)

Az ESET figyelmeztetése szerint a Kínához köthető Winniti APT csoport egy új backdoor felhasználásával Microsoft SQL (MSSQL) ellen indít támadásokat. A kollektíva legalább 2009 óta aktív, és elsősorban a repülésügyi, a játékpiaci, gyógyszeripari, technológiai, telekommunikációs és a szofver fejlesztési szektorok tekintetében végez kiberkémkedést. A „skip-2.0" nevet kapott, újonnan felfedezett malware lehetőséget biztosít a támadott MSSQL környezetben történő csendes megbújásra, miközben rejtett módon kapcsolatot létesít bármely fiókhoz egy „varázs jelszó" segítségével. A káros kód elsősorban MSSQL Server 11 és 12-es verziók ellen készült, amelyek jelenleg a legnépszerűbb verzióknak számítanak. A támadó egy sikeres hozzáférés után az adatbázison teljes körű módosítást hajthat végre.

A BSI szerint a Firefox a legbiztonságosabb böngésző

(zdnet.com)

A német Szövetségi Információbiztonsági Hivatal (BSI) biztonsági szempontból tesztelte a legnépszerűbb böngészőket, azonban ez csak a Mozilla Firefox 68 (ESR), a Google Chrome 76, a Microsoft Internet Explorer 11 és a Microsoft Edge programokra terjedt ki. A vizsgálat alapjául a BSI idén szeptemberben kiadott, webböngészőkre vonatkozó biztonsági ajánlása szolgált. Eszerint ahhoz, hogy biztonságosnak nevezhessünk egy böngészőt, annak egy sor követelményeknek meg kell felelnie, például ─ a teljesség igénye nélkül ─ támogatnia kell a TLS-t, a HTTP Strict Transport Security-t (HSTS, lásd: RFC 6797), a Sub-resource integrity-t (SRI), a Content Security Policy (CSP) 2.0-ás verzióját, emellett fejlett telemetriai és tanúsítványkezelési mechanizmussal kell rendelkeznie. A BSI szerint a vizsgáltak közül a Firefox az egyetlen, amelyik az összes kritériumnak megfelel.

A svéd rendőrség kémprogramokat használhat az erőszakos bűncselekmények gyanúsítottjai ellen

(securityaffairs.co)

A svéd kormány a kémprogramok használatának engedélyezését tervezi a bűnüldöző hatóságok számára. Ezek segítségével a hatóságoknak lehetősége lesz a gyanúsítottak elektronikai eszközein bonyolított titkosított kommunikáció megismerésére, az érintettek nyomon követésére, illetve az eszközök beépített mikrofonján és kameráján keresztüli megfigyelésre. A svéd belügyminiszter, Mikael Damberg október 22-én mutatta be Svédország eddigi legjelentősebb szervezett bűnözés elleni intézkedéscsomagját, amely 2020. március 1-től lép életbe. A 34 pontból álló program rövid és hosszú távú intézkedéseket, új hatásköröket és technikai eszközöket biztosít a hatóságok számára, emellett új szankciókat határoz meg az erőszakos bűncselekményekre vonatkozóan. **Bővebben...**

Tor böngésző 9.0 javított működéssel

(heise.de)

Új frissítést adtak ki a teljes anonimitást ígérő Tor böngészőhöz: A 9.0 verzió az első stabil kiadás, amely a Firefox 68 ESR-en (Extended Support Release) alapul. Az előző a 8.0-ás verzióban a fejlesztők elsősorban a felhasználói élményre összpontosítottak, a mostani kiadás azonban nagyobb hangsúlyt fektet a jobb működésre. Annak érdekében, hogy a böngésző működése intuitívabb legyen, változtatni kellett annak felépítésén és felületén. Eltűnt a „Hagyma gomb", amely korábban az eszközsoron volt. A böngésző címsorában található kis „i" szimbólum segítségével a felhasználó tájékozódhat a Tor-csatornáról (Tor Circuit) ─ azaz a webes útról ─, valamint egy gomb segítségével új csatornát is nyithat, a címsor jobb oldalán található „Új identitás használata" gomb segítségével pedig új identitást kérhet. **Bővebben...**