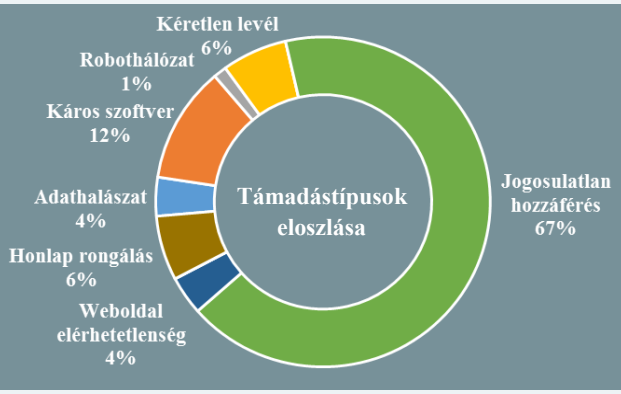
Incidens adatok: 2018.01.26. — 2018.02.01.



Kövessen minket online az itbiztonsag.govcert.hu oldalunkon, ahol naponta olvashatja legújabb híreinket!

Európai Adatvédelmi Nap és kapcsolódó ENISA-s kiadványok

(www.enisa.europa.eu)

Az ENISA is csatlakozott az Európai Tanács 47 országához az Európai Adatvédelmi Nap (European Data Protection Day) 12. évfordulójának megünnepléséhez 2018. január 28-án. Az ügynökség ennek kapcsán (is) igyekszik hangsúlyozni a 'privacy-by-design' szemléletet, valamint a személyes adatok biztonságos feldolgozása terén végzett kutatásainak eredményeit. Legfrissebb jelentésében ("ENISA report on privacy and data protection in mobile apps") az alkalmazás-fejlesztői környezet jellemzőivel és a GDPR technikai implementációjával foglalkozik. A jelentés kiemeli, hogy olyan bővíthető módszertanokra és bevált gyakorlatokra van szükség, melyek segíthetnek az adatvédelmi követelmények, a korszerű alkalmazás-tervezésbe való integrálásában. Emellett az "ENISA handbook on security of personal data processing" képében gyakorlat orientált esettanulmányokkal egészítette ki a korábbi kis- és középvállalkozások számára készült kockázatkezelési és biztonsági intézkedéseket tartalmazó anyagát is. **Bővebben...**

Kibertámadás is válthat ki nukleáris háborút?

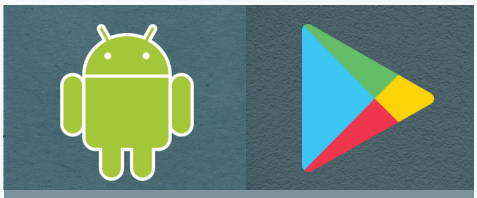
(www.nytimes.com)

Az Egyesült Államok új nukleáris stratégiájára vonatkozó javaslat lehetőséget biztosítana nukleáris válaszcsapásra amerikai infrastruktúrákat ért, nem-nukleáris támadások esetén is. A még engedélyezés alatt álló tervezet szakítana az évtizedek óta uralkodó koncepcióval, miszerint szigorúan limitált körülmények – például egy biológiai támadás – fennállása esetén lehet csak atomfegyvert alkalmazni egy megtorló művelet során. Az új elképzelés már jóval szélesebb körben értelmezi ezt, így az elektromos ellátórendszert vagy a kommunikációs rendszereket ért támadás is elegendő indok lehet. Ugyan a kibertámadásokat szó szerint nem nevesíti a múlt héten kiszivárgott dokumentum, azonban néhány korábbi és jelenlegi kormányzati tisztviselő – nem hivatalosan – megerősítette, hogy azok is beleesnek a radikális lépést potenciálisan kiváltó "extrém körülmény" kategóriájába, hangsúlyozva azonban, hogy jóval konvencionálisabb lehetőségek is adottak. **Bővebben...**

Ideje tekintetbe venni a GPS zavarók okozta fenyegetést is

(www.theregister.co.uk)

Az Egyesült Királyság kormányának tudományos irodája (Government Office of Science) egy régóta várt jelentésében megállapította, hogy a brit állami kritikus infrastruktúra és a sürgősségi szolgáltatók (rendőrség, tűzoltóság, mentők) GPS technológiától való függősége aggasztó mértéket öltött. A tanulmány feltárta, hogy több közszolgáltatás is erősen kitett a GPS technológiának, és különböző lépéseket javasolt annak érdekében, hogy növeljék a kritikus szolgáltatások GPS zavarás ellen tanúsított ellenálló képességét. Jelentésükben fenyegetésként azonosították a GPS jelek zavarását és meghamisítását. A GPS technológiát ráadásul nemcsak a közszolgáltatások használják, de például a pénzügyi szektor is, így beláthatatlan következményekkel járna egy erős GPS zavaró aktiválása London belvárosában – állapítja meg a jelentés. **Bővebben...**



Egyre több káros alkalmazást tilt ki a Google

(www.bleepingcomputer.com)

A tech óriás 2017 során több, mint 700 000 rossz, vagy rosszindulatú alkalmazást távolított el a Play Áruházból, ami a megelőző évhez képest 70%-os növekedést jelent - derült ki a Google kedden nyilvánosságra hozott éves összefoglalójából. A Google Play termékmenedzsere, Andrew Ahn a jelentésben arra is kitért, hogy a legtöbb eltávolított alkalmazás egy népszerű program kompromittált változata volt, ugyanis a támadók figyelemmel kísérik a keresések során megadott kulcsszavakat. Többek között gyakoriak voltak a fertőzött pornográfés a szélsőséges tartamú appok, ezekből a tavalyi év során 10 000-et távolítottak el az Áruházból. A Google Play Protect bevezetése óta megfigyelhető, hogy egyre kevesebb problémát okoznak az ún. 'potenciálisan káros alkalmazások' (Potentially Harmful Applications - PHA), amelyek száma a 2016-os évvhez képest tizededére csökkent. **Bővebben...**

IT biztonsági Tanács

Tartózkodjunk az online szolgáltatásokra történő regisztráció során a szervezeti e-mail címünk használatától. A belső informatikai biztonsági szabályzatnak megfelelően azokat kizárólag munkavégzésre, valamint kapcsolattartásra használjuk.

Amennyiben mégis szükséges szervezeti e-mail címünkkel regisztrálni, abban az esetben javasolt eltérő jelszó alkalmazása, ezzel csökkentve egy lehetséges kompromittálódás kockázatát.

Jövendő kiberbiztonsági feladatok

(www.enisa.europa.eu)

Az ENISA a kulcsfontosságú technológiai fejlesztésekről és azok biztonsági vonatkozásairól készített jelentést, melynek fő célja egy hivatkozási alap megteremtése a jövőbeli javaslatokhoz. Ennek érdekében áttekinti és azonosítja a technológia terén felmerülő főbb témaköröket és trendeket, úgy, mint az IoT, az autonóm rendszerek, az újgenerációs virtualizált infrastruktúrák (SDN, 5G), a virtuális és kiterjesztett valóság, az IoBNT (Internet of Bio-Nano things), a technológia hatása a társadalmakra, az MI és a robotika. Mindezek figyelembevételével a kiberbiztonsággal kapcsolatos lényeges aspektusok és kérdések is meghatározásra kerültek, amelyekkel az IT-biztonsági szakterületnek meg kell birkóznia. Eszerint fókuszba kell kerülnie – többek között – egy egységes tanúsítási rendszer kidolgozásának, a kibertérben végzett műveletek koordinálásának, a teljes technológiai életciklus biztonsági támogatásának, illetve például a végfelhasználók nagyobb bevonásának a biztonsági közösségbe. **Bővebben...**

A brit energiaszektor elleni támadás előkészítésével vádolják Oroszországot

(www.securityweek.com)

Gavin Williamson brit védelmi miniszter az Egyesült Királyság kritikus infrastruktúrái utáni kémkedéssel vádolja Oroszországot, amelyet egy átfogó támadási terv részének tekint. A Daily Telegraph-nak szokatlanul vészjósló hangon nyilatkozó miniszter elmondta, Moszkva különösen nagy érdeklődést mutat a brit energiaellátás iránt, kiterjedten tanulmányozzák és dokumentálják például a szigetország interkontinentális elektromos átviteli vonalait. Úgy véli mindezen tevékenységek egy olyan zűrzavarkeltő támadást készítenek elő, ami potenciálisan emberéleteket is követelhet, és ezt tartja jelenleg az országot érő legnagyobb fenyegetésnek. Korábban Ciaran Martin, a brit nemzeti kibervédelmi központ (National Cyber Security Centre) vezetője nyilatkozott hasonló témában. Szerinte elkerülhetetlen, hogy a brit kritikus rendszereket két éven belül támadás érje. **Bővebben...**

Amerikai ATM-ek támadás alatt

(bleepingcomputer.com)

A világ legnagyobb ATM gyártói közül ketten is (Diebold Nixdorf és az NCR Corporation) biztonsági figyelmeztetést adtak ki, mivel pénzkiadó automatáikat ún. "jackpotting" támadás érte az Egyesült Államokban. A gyűjtőfogalom alatt olyan technikákat értünk, amelyekkel a támadók fizikai hozzáférés során illegális pénzkiadásra tudják rávenni az ATM-eket. A Diebold Nixdorf gyártó szerint az alkalmazott metódus hasonlósága miatt feltételezhetően ugyanaz a csoport állhat a mostani akciók mögött, mint akik 2017 októberében Mexikóban végeztek ilyen támadásokat. Ezek során, amennyiben hozzáférnek az ATM hátoldalához, kicserélik az eszköz merevlemezét egy fertőzöttre, majd egy endoszkóp segítségével egy belső reset gombot megnyomva újrabootolják az eszközt, amelyen ezek után már kontrollt is nyertek. A cég szerint ez az eljárás csak a régebbi Opteva terminálokon működik. **Bővebben...**