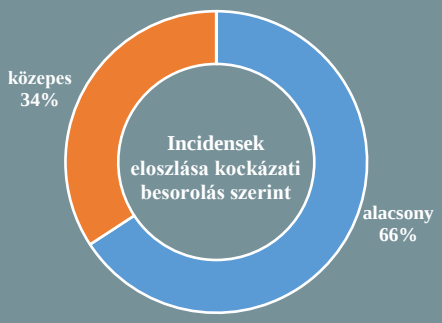
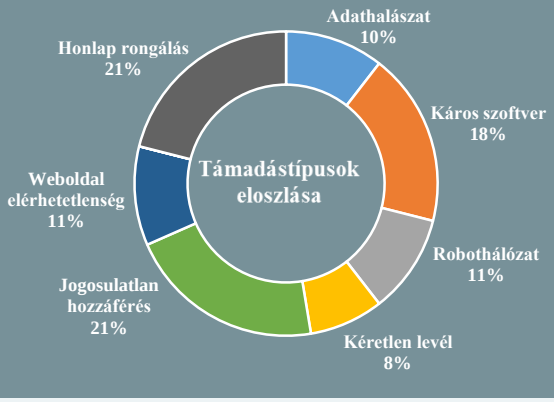
Incidens adatok:
2017.06.14. — 2017.06.20.





A TrendMicro egy újfajta kibertámadási stratégiára hívja fel a figyelmet

(blog.trendmicro.com)

A BPC-ként (Business Process Compromise) elnevezett eljárással máris hatalmas károkat okoztak (lásd a Bangladesh Bank elleni támadás), ami minden valószínűség szerint a jövőben csak nőni fog. Szemben a BEC-típusú (Business Email Compromise) támadásokkal – amelyek jellemzően a célkeresztben lévő szervezet egy kiválasztott munkatársát direkt módon próbálják rávenni valamilyen pénz kifizetésére vagy érzékeny adat megosztására – a BPC, a szervezet üzleti folyamatainak felderítésén és azok módosításán keresztül fejti ki hatását. Az ilyen támadások detektálása nagy körültekintést igényel, ennélfogva a felkészülést a szervezet biztonsági stratégiájának részévé kell tenni. **Bővebben...**

Észak-Korea állhat a 'Hidden Cobra' mögött

(www.forbes.com)

Az Egyesült Államok belügyminisztériuma és az FBI közös közleményében az észak-koreai kormányzatot teszi felelőssé több, 2009-óta felmerült kibertámadásért. A vádak szerint a 'Hidden Cobra'-ként azonosított (más néven Lazarus Group) hacker csoport áll több, a médiát, légügyi rendszereket, pénzügyi szektort és kritikus infrastruktúrát ért támadásért, amelyekre a jövőben is számítani kell. A csoport több malware családot is alkalmaz a támadásokhoz, ezek közül emelték ki a 'DeltaCharlie'-t, amelynek segítségével pusztító DDoS támadásokat lehet kivitelezni. **Bővebben...**

GDPR: az Egyesült Királyság rosszul áll a felkészülésben

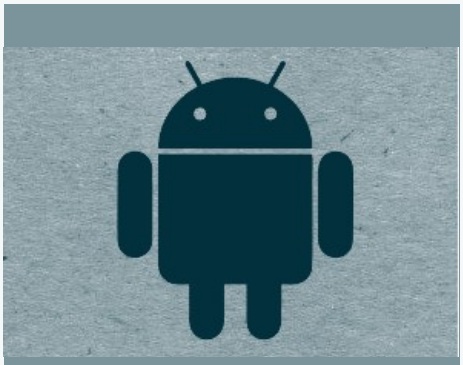
(www.helpnetsecurity.com)

Egy új felmérés szerint a brit vállalatok mindössze 6%-a foglalkozik kiemelten a GDPR-nak való megfeleléssel. Számukra a ’Brexit’ miatt is összetettebb a kérdés, a válaszadó vállalatok 26%-a jelezte, hogy nem egyértelmű számukra, hogy a kilépés után mennyiben kell megfelelniük az uniós követelményeknek. A probléma azonban nagyobb volumenű: ha a további vizsgált országok (Franciaország, Belgium, Luxemburg) válaszait is figyelembe vesszük, a szervezetek összesen több mint fele (55%) bizonytalan volt azzal kapcsolatban, hogy a határidőig eleget tud-e tenni a követelményeknek. **Bővebben...**

Egy új adathalász technika

(www.komando.com)

A támadók egyre jobban fókuszálnak a mobil eszközökre és egy új technika, az ún. 'URL padding' felhasználásával az adathalász SMS-ek (smishing) még veszélyesebbé válhatnak. A támadás során az áldozat egy látszólag legitim forrásból érkező (például Facebook, bankintézetek) üzenetet kap, amely egy szintén legitimnek látszó, azonban káros hivatkozást tartalmaz. A megtévesztés abból áll, hogy a linkre való kattintás után megnyíló káros oldal URL-jében kötőjeleket helyeznek el ami – a mobil böngészők címsorának rövidségét kihasználva – a valódi domain-t elfedi, így a felhasználó nem látja a cél webhelyet. Az ilyen támadások ellen leginkább fokozott figyelemmel lehet védekezni, például annak az észben tartásával, hogy egy bank soha nem kéri ügyfele biztonsági kódját. **Bővebben...**



Illegális kémkedés
(www.theregister.co.uk)

Mexikói non-profit szervezetek nyomozást kezdeményeztek egy kiberkémkedési kampány után, amely állami korrupcióról cikkező újságírók, emberjogi aktivisták és jogászok ellen irányult. A vizsgálatba bevont kanadai 'CitizenLab' által végzett technikai analízis során kiderült, a támadásokat az izraeli NSO Group-tól vásárolt 'Pegasus' nevű, mobilkészülékek ellen fejlesztett kiberfegyver segítségével hajtották végre. A támadások hátterében a mexikói kormányt sejtik, mivel az alkalmazott támadó infrastruktúráról ismert, hogy a gyártó cég kizárólag kormányoknak teszi azt elérhetővé. Az elemzők szerint szinte biztos, hogy törvényi engedély nélkül történtek a támadások. **Bővebben...**

IT biztonsági tanács

A hamis hírkampányok sikere sok esetben a felhasználók figyelmetlenségének köszönhető.

Néhány dolog, ami kételyt ébreszthet bennünk a hír valódiságával kapcsolatban: túlzó, hatásvadász címek; egy valós portál nevéhez hasonlító webcím; forrás, szerző megjelölésének hiánya; hibás vagy hiányzó dátummegjelölés; elgépelések a szövegben; halmozott írásjelek használata; igénytelen, webdesign.

Az ENISA nagyobb támogatásért folyamodik
(www.euractiv.com)

Az Európai Unió kiberbiztonsági ügynöksége szeptemberben átalakuláson fog átesni, amikor az Európai Bizottság megújítja a megbízását. Az athéni központú szervezet nagyobb büdzsét szeretne, hogy lépést tudjanak tartani az egyre gyakoribb fenyegetésekkel és támadásokkal. Udo Helmbrecht igazgató szerint a legfőbb probléma az, hogy még mindig nincs egy egységes eljárásrend arról, hogy az európai hatóságok hogyan birkózzanak meg egy kiberbiztonsági krízissel. Az ENISA ezen kíván változtatni. **Bővebben...**

Egy brit hacker betört az amerikai katonai szatelit hálózatba
(www.theregister.co.uk)

Az amerikai Védelmi Minisztérium állítása szerint 628 000 dollárba került a betörés kivizsgálása és a kármentesítés. A 25 éves Sean Caffrey elismerte, hogy több, mint 800 felhasználó e-mail címét és felhasználónevét, valamint körülbelül 30 000 műholdas telefonszámot szerzett meg 2014 júniusában. Az adatszerzés módszerét még nem hozták nyilvánosságra**. Bővebben...**

Nemzetbiztonsági veszélyt hordozó technológiatranszfer
(www.bbc.com)

A BBC Arabic és egy dán lap bizonyítékot talált arra vonatkozóan, hogy az Egyesült Királyság egyik legnagyobb védelmi vállalata, a BAE Systems, nagy mennyiségben értékesített megfigyelő technológiát, a Közel-Keleten. Habár ezek a tranzakciók legálisak voltak, olyan technológiák is érintettek – mint például az 'Evident' kriptoanalízis funkciókkal bíró webes megfigyelő szoftver – amelyeket potenciálisan az Egyesült Királyság és szövetségesei ellen is felhasználhatnak. **Bővebben...**

A legvalószínűbb, hogy egy e-maillel kezdődik
(digitalguardian.com)

A kibertámadások 91%-a adathalász e-maillel indulhat, állítja a PhishMe legújabb kutatása. Erre az eredményre közel 40 millió szimulált adathalász e-mail kiküldésével és az azokra érkezett válaszok elemzésével jutottak. Az adathalászat mára egészen szofisztikált módszerekkel történik, a PhisMe kutatása azonban rámutatott, hogy a vállalatok még a legalapvetőbb technikákkal szemben is sérülékenyek. További érdekes adat, miszerint a válaszolási arány az egészségügyi szektorban volt a legnagyobb. **Bővebben...**

1 millió dollárnyi váltságdíj kifizetés Bitcoinban
(securityweek.com)

A dél-koreai Nayana web hosting cég 153 Linux szerverét ért ransomware támadásban több mint 3 400 kisvállalalti ügyfél adatai kerültek titkosításra. Az adatok visszafejtéséhez eredetileg 550 Bitcoin váltságdíjat követeltek a támadók, ám végül 397,6 Bitcoin-ban állapodtak meg. A cég tájékoztatása szerint az összeg kifizetése és ezzel együtt az adatok visszafejtése három részletben történik, amelyből kettő már le is zajlott. A Trend Micro úgy véli a támadáshoz az 'Erebus' kártevőt használták fel, amely egy nagyon kifinomult titkosítási módszert alkalmaz, így a visszafejtés az RSA kulcsok nélkül nem lehetséges. **Bővebben...**