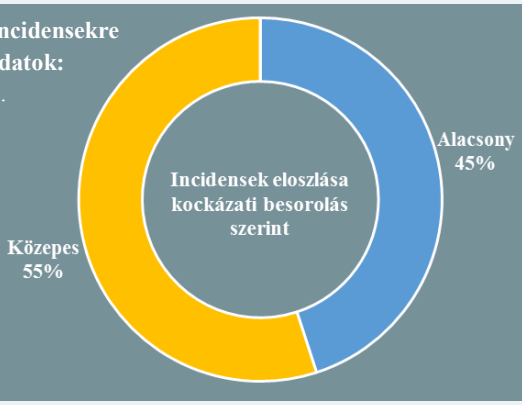
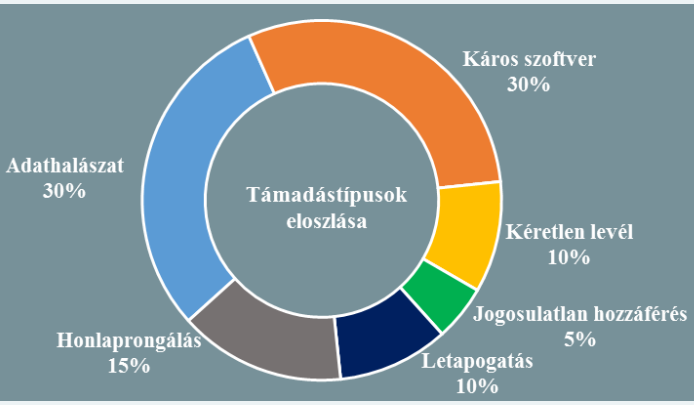
Az NKI által kezelt incidensekre vonatkozó statisztikai adatok:
2018.08.31. - 2018.09.06.





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

A lengyel parlament elfogadta a NIS irányelvet implementáló törvényt

(www.ik.org.pl)

A hálózati és információs rendszerek biztonságáról szóló Európai Uniós irányelv alapján a kiberbiztonsági rendszer részét képezik a kritikus szektorokban ─ mint például az energia-, a szállítás- és az egészségipar ─ ún. alapvető szolgáltatásokat nyújtó szereplők, a digitális szolgáltatók, a hálózatbiztonsági vészhelyzeteket elhárító csoportok (CSIRT/CERT-ek), egy kiberbiztonsági szabályozó szerv ─ ami az elsődleges kapcsolati pont funkciót is ellátja ─ valamint egy tanácsadó testület, amely a kiberbiztonsággal összefüggésben lévő kérdésekkel foglalkozik majd. A most elfogadott törvény az incidensekre történő reagálási feladatokat a lengyel kibertérrel összefüggésben három szervezet között osztja fel, eszerint a lengyel Belbiztonsági Ügynökség irányítása alatt álló CSIRT GOV felügyeli a kritikus infrastruktúrákat és kormányzati rendszereket, a NASK állami kutatóintézet által működtetett CSIRT NASK-hoz a magánszektor és felsőoktatás tartozik majd, a Nemzetbiztonsági Minisztérium felügyelete alatt álló CSIRT MON pedig elsősorban a katonai és kiemelt gazdasági szereppel bíró szervezetek esetében lát el incidenskezelési feladatokat. **Bővebben...**

Kibertámadások keresztttüzében Svédország röviddel a választások előtt

(www.chron.com)

Egy svéd védelmi kutatóintézet (FOI) által készített jelentés szerint egyre több automatizált fiók jelenik meg a Twitteren, amelyeken keresztül a kormányon lévő Szociáldemokrata Párttal szemben a bevándorlásellenes nacionalista pártot (Svéd Demokraták) támogatják hamis hírekkel. A Svéd Biztonsági Szolgálat (Säpo) szerint emellett a kormányzati szerveket és politikai csoportokat célzó kibertámadások száma is megemelkedett. Ugyan a zavarkeltés mindeddig inkább járulékosnak tekinthető ─ valamint nem is minden esetben köthető külföldi hatalomhoz vagy a választásokhoz ─ a szolgálat nagyobb erőfeszítéseket tesz a szeptember 9-én esedékes választások védelmének biztosítására ─ mondta Linda Escar, a szerv egyik helyettes vezetője, a Swedish Radio-nak. **Bővebben...**

Önkéntes alapon vár titkosítást megkerülő megoldásokat a Five Eyes

(www.homeaffairs.gov.au)

Az ún. „Öt szem” (Five Eyes) hírszerzési nemzetszövetség a titkosítás kapcsán új alapelveket fogadott el. Elsőként kiemelik, hogy a törvényes úton történő adatgyűjtés nem csupán a kormányok feladata, hanem minden ágazati szereplő kölcsönös felelőssége, ennek kapcsán pedig a technológiai szolgáltatók részéről nagyobb közreműködésére számítanak. Az információk begyűjtése során azonban alapvető fontosságúnak ítélik az eljárás tisztességes lebonyolítását, a mindenkor szükséges független külső hatósági és/vagy bírói felügyelet. A digitális szolgáltatókat pedig önkéntes alapú hozzáférési megoldások kialakítására bátorítják, és ahelyett, hogy konkrét technikai követelményeket fogalmaznának meg, szabad kezet adnak a megvalósításban. **Bővebben...**

ENISA riport a 2017-es incidensekről

(www.enisa.europa.eu)

Az ENISA közzétette a 2017-es évben történt telekommunikációs szektorbeli incidenseket összefoglaló jelentését, amely szerint tavaly mintegy 169 incidenst jeleztek a nemzeti telekommunikációs szabályozó hatóságok (NRA-k). A korábbi évek trendjeinek megfelelően a legtöbb incidens (62%) most is valamilyen rendszer hiba ─ többnyire hardveres ─ miatt következett be. Az esetek 17%-ban természeti tényező, 22%-ban pedig áramkimaradás volt a felelős, szándékos károkozás ─ DDoS támadás, vagy például kábellopás ─ azonban az összes esemény csupán 2%-át érintette. **Bővebben...**

Az Apple új portálon adna ki felhasználói adatokat a hatóságoknak

(www.9to5mac.com)

Az Egyesült Államok Szenátusának írt levelében az Apple egy olyan új webes portál fejlesztését ismertette, amely egyszerűsítené a bűnüldöző hatóságok számára a felhasználói adatokhoz való hozzáféréseket. A tavalyi évben közel 14.000 hozzáférési kérelem érkezett a hatóságoktól, ezért a cég a korábban erre a célra használt email alapú rendszer frissítését kívánja megvalósítani, amely - bírói határozat birtokában - lehetővé tenné az adatokhoz való hozzáférésekre vonatkozó kérelmek benyújtását, a kérelmek aktuális állapotának figyelemmel kísérését, valamint az Apple által szolgáltatott adatok elérését. A portál mellett az Apple egy olyan speciális csapat létrehozását is tervezi, amely a világszerte működő bűnüldöző hatóságok számára tartana képzéseket arra vonatkozóan, hogy a cég miként képes kezelni az ilyen jellegű helyzeteket. **Bővebben...**

IT biztonsági Tanács

A fiatalkorú gyermekek online védelme érdekében érdemes átgondolni, milyen telepített alkalmazásokhoz engedünk hozzáférést gyermekeink számára. A következőkre odafigyelve csökkenthető a nemkívánatos tartalmakkal való találkozás esélye:

- Az alkalmazás legyen reklámmentes;
- Korlátozott tartalommegjelenítéssel bírjon, amire a készítő garanciát is vállal;
- Ne legyenek rejtett funkciók (pl.: vásárlási lehetőség);
- Keressük a korhatár-besorolási rendszer alapján a megfelelő PEGI számot;

SSL tanúsítványok buktattak le darknetes oldalakat

(www.bleepingcomputer.com)

Egy biztonsági kutató szerint több olyan Tor oldal is fellelhető, amelyek hibás konfiguráció miatt SSL tanúsítványaikon keresztül felfedhetik a publikus IP címeiket. A darknetes oldalakat kiszolgáló szervereket ugyanis az oldalak anonimitásának megőrzése érdekében úgy szokás beállítani, hogy kizárólag a lokálhoszton (127.0.0.1) „hallgatózzanak”, azonban előfordul, hogy az oldal adminisztrátora ezt elmulasztja megtenni, és azok bármilyen külső IP címről fogadnak kéréseket. Amennyiben egy ilyen site SSL tanúsítvánnyal rendelkezik, annak CN mezője tartalmazza a Tor hálózatbeli (onionos) címét, innentől kezdve a szerver publikus IP címe és a „darknetes” címe között kapcsolat állítható fel. **Bővebben...**

A Google megszabadulna az URL-ektől, de még nem tudja hogyan

(www.wired.com)

A Chrome biztonsági csapata egy új ajánláson dolgozik, amely azt az ambiciózus célt tűzte ki maga elé, hogy a webes URL-ek helyett egy alternatív megoldást dolgozzon ki, mivel azok mára nagyon bonyolulttá és nehezen értelmezhetővé váltak, ez pedig csak a felhasználókat megtéveszteni igyekvő kiberbűnözőknek kedvez. Adrienne Porter Felt, a Chrome műszaki menedzsere elmondta, az új URL megjelenítési mód célja, hogy a webes identitás igazolása jóval egyszerűbbé váljon, és a felhasználók egyértelműen meg tudják állapítani, hogy megbízhatnak-e a meglátogatott oldalban. A Chrome csapata évek óta foglalkozik az URL-ek biztonsági problémájával, 2014-ben például azt javasolták, hogy alapértelmezetten csak a domain kerüljön megjelenítésre, és amennyiben valakit érdekel a teljes URL, azt az ún. „eredet chipre” kattintva érhesse el. **Bővebben...**

Új funkciónak hitték a Twitter programhibáját

(www.mashable.com)

A Twitter közösségi média alkalmazás egy hibájának köszönhetően a felhasználók azt tapasztalták, hogy bizonyos esetekben úgy tűnt, mintha olyan bejegyzéseket is kedveltek volna, amelyeket eredeti szándékuk szerint nem jelöltek volna be. A Twitter szóvivője szerint sok felhasználó érintett a hibában, ami kifejezetten az idővonalakra korlátozódik, ugyanis a kedvelések listája között már nem jelennek meg a bejegyzések. A hibajelenség a közösségi média szereplőinek csak egy kisebb részére korlátozódok, és akkor érhető tetten, ha egy felhasználó, akár véletlenül is kedvelt egy bejegyzést, de aztán ezt a jelölést visszavonta. Ilyenkor egyes esetekben továbbra is úgy szerepelt az eredeti bejegyzés az idővonalon, mintha azt a felhasználó kedvelte volna. **Bővebben...**

Az IoT eszközök biztonsága továbbra sem az elsődleges szempont

(www.helpnetsecurity.com)

A Trend Micro által publikált tanulmány szerint a vállalatok világszerte nem vonják be az IT biztonsági csapatokat az ipari IoT projektekbe. A felmérésben résztvevő informatikai és biztonsági döntéshozók bevallása szerint a megoldások kiválasztásánál 79%-uk támaszkodik az informatikai részlegre, és mindössze csupán 38%-uk vonja be a biztonsági csapatot. Kevin Simzer a Trend Micro vezérigazgatója szerint a sebezhetőségek többsége abból ered, hogy a projektek kezdeti lépéseiben a szervezetek számára továbbra sem élvez prioritást a biztonság, ezért a tervezéskor nem számolnak az eszközök frissítési és javítási szükségleteivel. **Bővebben...**