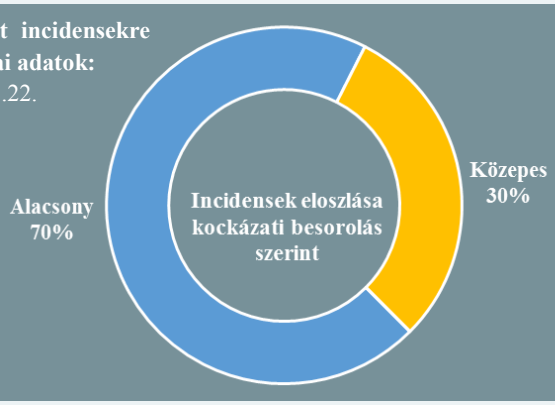
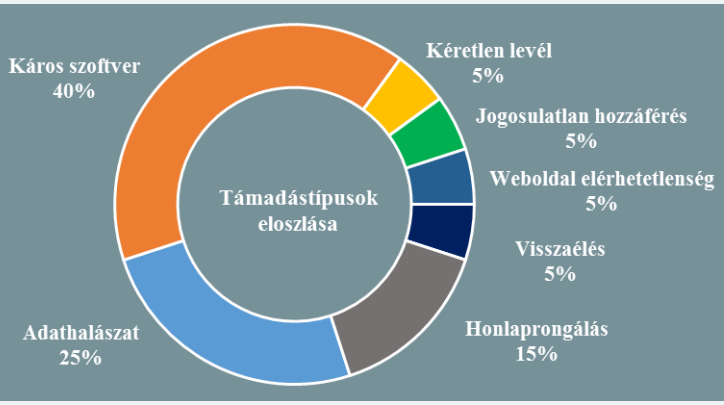
NEMZETI KIBERVÉDELMI INTÉZET
GOVCERT

Nemzetközi IT-biztonsági sajtószemle

2018. 47. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok:
2018.11.16. - 2018.11.22.





Kövessen minket online az itbiztonsag.govcert.hu oldalunkon!

Egyre népszerűbbek az anonimitást biztosító internetes keresők

(securityweek.com)

A nagy tech vállalatok adatgyűjtési tevékenységét érő komoly kritikák, valamint az európai szabályozás szigorodása miatt egyre népszerűbbek a felhasználók privát szféráját tiszteletben tartó kisebb európai kereső szolgáltatások, mint például a Mojeek, a Qwant, az Unbubble, vagy a Swisscows. Eric Leandri, a párizsi székhelyű Qwant elnöke elmondta, számukra a felhasználók magánélethez való jogának tiszteletben tartása alapvetés, szemben a tengerentúlon uralkodó hozzáállással, ahol az internet felhasználókra hajlamosak úgy tekinteni, mint olyan fogyasztókra, akik jogait az adott szolgáltatási szerződés határozza meg. A Qwant legnagyobb piacán, Franciaországban jelenleg 6%-os részesedéssel bír, havonta átlag 80 milliós látogatással, legutóbb pedig már a francia hadsereg és a parlament is jelezte, hogy saját rendszereiken ezt teszik alapértelmezetté. Míg a Qwant saját indexelést végez, olyan szolgáltatások is elérhetők ─ például a holland startpage.com ─ amely anonimizálja a Google keresési eredményeit. Mindezek mellett a keresések háromnegyede továbbra is a tech óriás szolgáltatásán keresztül zajlik, így a cég piaci fölénye megkérdőjelezhetetlen.

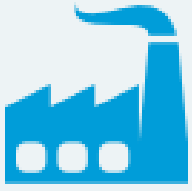
Megszemélyesítésre adott módot a német e-személyivel történő webes autentikáció hibája

(www.zdnet.com)

Biztonsági kutatók sérülékenységet tártak fel egy német állami portálok által elektronikus személyi igazolvánnyal történő webes bejelentkezések kezelését végző szoftver komponensben (Governikus Autent SDK); a biztonsági hiba kihasználásával lehetőség nyílt más állampolgárok nevében történő bejelentkezésre az érintett site-okon. A problémát csak most nyilvánosságra hozó SEC Consult azt már 2018 júliusában felfedezte, a detektálást követően pedig azonnal értesítette a CERT-Bundot, a gyártói hibajavítás így már augusztusban megtörtént. Az esetről tudósító ZDNet hivatalos megkeresés útján igényelt információt a német Szövetségi Informatikai Biztonsági Hivataltól (BSI) azzal kapcsolatban, hogy a német kormányzati portálokon telepítették-e a hibajavítást, illetve, hogy az érintett weboldalak autentikációs naplóbejegyzéseit átvizsgálták-e a szóban forgó sérülékenység kihasználásának nyomai után kutatva.

A kritikus ipari rendszerek esetében félrevezetőek lehetnek a CVSS pontszámok

(www.securityweek.com)



A sérülékenységek súlyosságának meghatározására használatos nemzetközi CVSS pontozási rendszer az ipari irányítástechnikai- és vezérlőrendszerek (ICS – Industrial Control Systems) esetében félrevezető lehet, ami negatív következményekkel járhat a szervezetekre nézve ─ mutatott rá Ilan Barda, a Radiflow vezérigazgatója egy kiberbiztonsági konferencián. Véleményét több kiberbiztonsági szakértő is osztja, például Moreno Carullo, a Nozomi Networks társalapítója és vezérigazgatója, aki a pontszámítási rendszer előnyeinek elismerése mellett is úgy véli, azt inkább csak iránymutatásra kellene használni, és alapvetően mindenkinek a saját környezetéhez mérten magának kell meghatároznia egy adott sérülékenység súlyosságát. **Bővebben...**

Több, mint félmillió áldozata van egy androidos malware-nek

(www.techcrunch.com)

Az ESET kutatói felfedeztek 13 olyan, a Google Play-ről letölthető káros alkalmazást, amelyek autóvezető játékoknak álcázták magukat, azonban megnyitáskor egyetlen tevékenységet végeztek: káros kódot töltöttek le a háttérben. A malware pontos tevékenységéről nem közöltek információkat, azonban annyi biztos, hogy az hozzáférést szerez az eszköz teljes hálózati forgalmához, ami a kód gazdájának privát információk megszerzésére adhat módot. A Google már gondoskodott az alkalmazások eltávolításáról, azonban az esetről posztoló kutató szerint a szóban forgó appokat összesen így is mintegy 580 000-en telepítették. A tech óriás tavaly több, mint 700 000 káros alkalmazást törölt a Google Play-ről.

IT biztonsági Tanács

Az ünnepi szezon idején legyünk fokozottan figyelmesek az internetes vásárlások során, ugyanis ezen időszakban jelentősen elszaporodhatnak a rosszindulatú kódokat, hamis hirdetéseket terjesztő, vagy személyes adatokat eltulajdonító weboldalak és applikációk.

Az alkalmazások megbízható forrásból (Google Play, App Store) történő letöltése esetén is ellenőrizzük az alkalmazások fejlesztőit és a felhasználói véleményeket, valamint az alkalmazás által kért jogosultságokat.

A weboldalakat soha ne üzenetben kapott linkre kattintva nyissunk meg, hanem a címeket manuálisan begépelve, valamint mindig ellenőrizzük a feladót, illetve a webáruházat, amelynek szolgáltatásait igénybe kívánjuk venni.

Célzott adathalász kampány folyik orosz pénzügyi szervezetek ellen

(www.bleepingcomputer.com)

Rendkívül szofisztikált adathalász támadási kampány indult orosz bankok ellen, amelynek hátterében a Silence névre keresztelt csoportot sejtik, akik a feltételezések szerint legitim információbiztonsági háttérrel bírnak, valamint különböző valós pénzügyi dokumentációkhoz is hozzáférnek. Az orosz központi bankot megszemélyesítő megtévesztő e-mailek ugyanis a Group-IB információbiztonsági cég szerint szinte megkülönböztethetetlen módon hasonlítottak az eredetiekre. A kiberbiztonsági cég az eset kivizsgálásáról készített jelentése szerint a támadók célja a támadott bankok hálózatán olyan belső állomásokhoz történő hozzáférés volt, amelyek lehetővé tehetik a különböző pénzügyi tranzakciók kompromittálását. A jelentésből az is kiderül, hogy október végén a hírhedt MoneyTaker csoport is támadási kampányt indított, nagyon hasonló technikát alkalmazva. A Group-IB e két kollektívát a nemzetközi pénzügyi szervezetek számára legnagyobb veszélyt jelentő csoportok között tartja számon.

Átfogó ENISA tanulmány az ipari IoT eszközök biztonságának növeléséhez

(www.enisa.europa.eu)

A már zajló 4. ipari forradalom szorosan összekapcsolódik a kiberbiztonsággal, az egyre nagyobb számban előforduló biztonsági események pedig komoly hajtóerőt jelentenek az ellenálló képesség növeléséhez. Az ENISA friss tanulmányában azon automatizált rendszerekkel dolgozó ipari cégek számára fogalmaz meg javaslatokat és biztonsági megoldásokat, amelyek ipari IoT berendezéseket alkalmaznak, vagy terveznek használni. Az összefoglaló többek között definiálja a releváns terminológiákat ─ mint például az Ipar 4.0, okos gyártás, ipari IoT ─, rendszerezi a digitális ipari asseteket, valamint támadásokon és kockázatokon alapuló átfogó fenyegetési taxonómiát vezet be. A teljességre törekvő anyag összeállításakor az ügynökség szem előtt tartotta, hogy az IoT eszközök teljes életciklusát végigkövesse biztonsági szempontból.

Kibertámadás ért egy olasz közigazgatási informatikai rendszert

(www.reuters.com)

Ismeretlen hackerek november 12-én illetéktelen hozzáférést szereztek több ezer olyan e-mail fiókhoz, amelyek a hivatalos iratok elektronikus kézbesítésére szolgáló Posta Elettronica Certificatához tartoznak ─ írja a Reuters. Roberto Baldoni, olasz állami kiber felelős szerint a támadás egy olyan Róma közelében található szervert ért, amely a közigazgatásban használt tanúsított e-mailek kezelését végzi. Ennek során mintegy félmillió fiók adatait szerezték meg, többek között bírákat és biztonsági tisztviselőket is kompromittálva ─ miniszterek, titkosszolgálati és katonai vezetők érintettsége jelenleg nem tisztázott. Baldoni szerint a külföldről indult támadás technikai szempontból nem volt kifinomultnak nevezhető, mégis komoly következményekkel járt, azonban mára úrrá lettek a problémán.

Megélénkült az FSB kiber-hírszerzési tevékenysége

(www.arstechnica.com)

Az ukrán állami CERT figyelmeztetést adott ki egy új Pterodo Windows backdoor variáns miatt, amelyet ukrán kormányzati ügynökségek ellen vetettek be. Védelmi tisztviselők mindezt egy nagyszabású támadás előkészítéseként értékelik, mivel a káros szoftver fő feladata rendszerinformációk gyűjtése és továbbítása távoli kiszolgálók felé. **Bővebben...**