ÚRAD PODPREDSEDU VLÁDY SR
PRE INVESTÍCIE
A INFORMATIZÁCIU

CSIRT.SK

TLP: White

Mesačná správa CSIRT.SK

September 2018

Uvažovali ste niekedy, či váš účet na Facebooku, Twitteri, e-mailová schránka na Google, alebo kdekoľvek inde je naozaj dobre zabezpečený? Čo ak bol hacknutý a útočníci ho využívajú na šírenie spamu, alebo vám z neho „vykradli“ citlivé osobné údaje? Čo ak by ich použili na krádež vašej identity, alebo vás nimi vydierali? Keď vezmeme do úvahy množstvo uniknutých databáz, ako napríklad obrovský počet napadnutých facebookových účtov tento mesiac (čítajte nižšie), sú to legitímne otázky. Niektoré spoločnosti zavádzajú pre svojich užívateľov možnosti, ako skontrolovať, ktoré zariadenia a odkiaľ sú k ich účtom pripojené. Stačí, ak vo svojom Twitteri nájdete položku 'Apps and sessions' v mobilnej aplikácii, alebo 'Apps and devices' na PC. Pre Facebook pozrite položku Settings/Security/‘Where You’re Logged In‘. Google pre zmenu ponúka túto informáciu vpravo na spodku e-mailovej schránky (Last account activity, Details). Chcete si overiť, že vaša e-mailová schránka, alebo heslo neboli kompromitované? Ako na to sa dozviete nižšie, v informácii s názvom „42 miliónov e-mailových adries a hesiel nájdených na bezplatnej službe zdieľania súborov“.

Keď hovoríme o bezpečnosti hesiel, spomeňme štúdiu spoločnosti Switchfast. Hovorí, že až 1 z 5 zamestnancov malých a stredných firiem zdieľa svoje heslá so spolupracovníkmi. Toto zistenie získali po komunikácii s vedúcimi pracovníkmi 600 firiem. Okrem toho len 24% vedúcich pracovníkov a 31% zamestnancov si aktivovalo dvojfaktorovú autentifikáciu. Z toho vyplýva, že pracovníci s prístupom k citlivejším informáciám ich chránia menej dôkladne, ako ostatní. Správa hovorí tiež o tom, že 91% útokov na firmy sa odohráva na báze phishingových e-mailov. Preto je potrebné pravidelne školiť zamestnancov o tejto hrozbe. Jedno zdanlivo nevinné kliknutie môže spôsobiť obrovské škody.
(https://blog.switchfast.com/switchfast-report-small-businesses-are-too-complacent-with-cybersecurity)

Dobrou voľbou ako posilniť informačnú bezpečnosť spoločnosti, je podľa štúdie Goode Intelligence zaviesť viacfaktorovú autentifikáciu s využitím biometrických údajov. Nejedná sa síce o neprelomiteľné zabezpečenie, no predmetná štúdia poukazuje na mnohé výhody jeho implementácie. Autentifikácia s využitím biometrických prvkov predstavuje zvýšený komfort zákazníkov/klientov, a zároveň zvýšenú úroveň bezpečnosti citlivých systémov.

Nielen ochrana prístupových údajov zabezpečí dôležité dáta pred kompromitáciou. Tento mesiac sme boli informovaní o reálnom pokuse o zneužitie zraniteľnosti v redakčnom frameworku Drupal, open source softvéri určenom na výstavbu webstránok. Útočníci si vytipovali zraniteľnú webstránku a pokúsili sa prevziať nad ňou kontrolu.

A tiež pamätajte – nezdieľajte citlivé materiály na verejných službách zdieľania súborov ako Google Drive, či ulož.to .

Riešené incidenty na Slovensku a z našej činnosti

CSIRT.SK nezaznamenal tento mesiac významný útok na infraštruktúru SR. V mesiaci september riešil prevažne phishingové kampane na svoju konštituenciu a informoval inštitúcie o napadnutí botmi. O zvýšenom počte phishingových kampaní požadujúcich finančný prevod sme písali na našej stránke (https://www.csirt.gov.sk/oznamenia-a-varovania-803.html?id=197).

Okrem toho informoval niektoré inštitúcie vo svojej konštituencii o kritickej zraniteľnosti MikroTik routerov (čítajte nižšie), nakoľko tieto zariadenia boli objavené na niekoľkých IP adresách daných organizácií.

CSIRT.SK vykonal aj niekoľko vyžiadaných penetračných testov webových stránok a systémov inštitúcií vo svojej konštituencii.

V septembri dostal CSIRT.SK informáciu o zdieľaní citlivej projektovej dokumentácie cez nezabezpečený Google Drive účet. Podľa informácie sa jednalo o opakovanú aktivitu. CSIRT.SK upozornil na potenciálne nebezpečenstvo zodpovedné osoby a navrhol možnosti, ako v budúcnosti riešiť zdieľanie súborov.

V rámci svojej analytickej činnosti sa zaoberal malvérom Pegasus a Remcos. Pegasus (jedná sa o odlišný malvér ako nižšie popísaný spyware) je bankový trójsky kôň, ktorý infikoval systémy najmä v ruských bankách. Jeho analýzu sme uverejnili na našej webstránke tu: https://www.csirt.gov.sk/aktualne-7d7.html?id=159 . Remcos je malvér typu RAT (remote administration tool), určený na prevzatie kontroly nad vzdialeným zariadením. V analýze, uverejnenej na našej stránke tu: https://www.csirt.gov.sk/aktualne-7d7.html?id=161 , sme rozobrali aj spôsob jeho šírenia a inštalácie.

Významné útoky vo svete

Tisíce MikroTik routerov odpočúvané

Kritická zraniteľnosť vo firmvéri routerov od firmy MikroTik umožnila útočníkom jednoduchým spôsobom získať prihlasovacie údaje do systémov týchto zariadení. Vďaka tomu útočníci aktívne odpočúvali vyše 7500 routerov MiktoTik. Ďalších 239 000 zariadení bolo napadnutých a pripravených k odpočúvaniu komunikácie a odchytávaniu dát. Zraniteľných bolo celosvetovo až 370 000 routerov.
O tejto zraniteľnosti sme písali vo varovaní na našej stránke (https://www.csirt.gov.sk/oznamenia-a-varovania-803.html?id=193).

Únik údajov o kreditných kartách klientov British Airways

Až 380 000 klientov British Airways bolo zasiahnutých kybernetickým útokom na túto spoločnosť. Uniknuté dáta predstavovali mená a adresy klientov spolu s číslami ich kreditných kariet. Zasiahnutí boli zákazníci, ktorí si rezervovali letenky cez stránku spoločnosti www.ba.com a cez ich mobilnú aplikáciu v intervale 21.8.-5.9.2018.

Veeam ponechala verejne dostupnú databázu klientov

Švajčiarska spoločnosť Veeam zaoberajúca sa vývojom aplikácií na zálohovanie, manažovanie a obnovu dát ponechala niekoľko dní verejný prístup k databáze MongoDB s približne 445 miliónmi záznamov o svojich zákazníkoch. Prístupné boli údaje ako mená zákazníkov, e-mailové adresy, IP adresy, krajiny pôvodu a veľkosti spoločností.

42 miliónov e-mailových adries a hesiel nájdených na bezplatnej službe zdieľania súborov

Takmer 42 miliónov e-mailových adries s heslami a čiastočnými údajmi o kreditných kartách bolo nájdených na bezplatnej službe zdieľania súborov kayo.moe. Pravdepodobne sa jedná o databázu určenú na tzv. credential stuffing útoky. Overiť si, či nastal prienik do Vašej e-mailovej schránky, si môžete napríklad v databáze, ktorú zozbieral bezpečnostný výskumník Troy Hunt, na stránke https://haveibeenpwned.com/. Overiť si môžete aj dostupnosť svojho hesla na https://haveibeenpwned.com/Passwords.

Feedify infikovaný skriptom na krádež dát MageCart

Služba Feedify je využívaná mnohými internetovými obchodmi, ktorým prináša možnosť interaktívnej komunikácie so zákazníkmi. V septembri oznámil výskumník s pseudonymom Placebo na svojom Twitteri, že do skriptov služby Feedify bol vložený škodlivý kód MageCart, určený na krádež platobných údajov obetí. Stránky využívajúce Feedify sa odvolávali na tieto skripty, a tak automaticky načítali aj spomenutý malvér. Takto bolo napadnutých vyše 4000 webstránok, čo ohrozilo celú ich klientelu.

Microsoft makrá sú stále najbežnejším vektorom útokov

Prieskum spôsobov šírenia malvéru, ktorý ešte v auguste vykonala spoločnosť Cofense, ukazuje, že Microsoft makrá sú najbežnejšou cestou, ktorú útočníci využívajú. Zodpovedali 45% analyzovaných spôsobov šírenia. Škodlivé súbory sú zväčša doručované e-mailom. Druhým najčastejším spôsobom bola zraniteľnosť v Microsoft Office z roku 2017 (CVE-2017-11882). Aj preto odporúčame neustále aktualizovať všetok nainštalovaný softvér.

Dve miliardy Bluetooth zariadení zraniteľných rok po zverejnení Blueborne sady chýb

Napriek tomu že súbor 9 zraniteľností nazvaný Blueborne bol zverejnený minulý rok, z odhadovaných 5,3 miliardy zariadení ostáva stále 2 miliardy neaktualizovaných. Pritom úspešným zneužitím by útočníci mohli získať úplnú kontrolu nad zariadeniami a dátami v nich uloženými. Mnohé zariadenia neumožňujú inštalovať aktualizácie, iné jednoducho neaktualizovali ich používatelia.

Microsoft odstránil z TechNetu 3000 podvodných reklám na technickú podporu

Vyše 3000 podvodných reklám ponúkajúcich služby technickej podpory odstránila spoločnosť Microsoft zo svojej stránky TechNet po tom, ako im objav nahlásil výskumník. Krátko po nahlásení však boli pridávané nové reklamy na podvodné služby. Podvodníci sa snažia získať týmto spôsobom dôveryhodnosť a zviditeľniť sa. Podobný trend zaznamenala aj spoločnosť Google. Filtrovanie takýchto reklám bude potrebné vykonávať špeciálnymi prostriedkami, ktoré spoločnosti vyvíjajú.

Smart TV Vizio sledovali svojich divákov...

Spoločnosť Vizio, vyrábajúca inteligentné televízory, čelila žalobe nahnevaných zákazníkov. 11 miliónov zariadení, ktoré vyrobili, malo totiž štandardne nastavené sledovanie svojich divákov. Televízory zaznamenávali vzory správania zákazníkov – útržky sledovaných programov spolu s dátumom, časom , kanálom a informáciou, či bol program sledovaný naživo, alebo z nahrávky. Zbierali tiež dáta zo služieb ako Netflix, DVD médií, a tiež streamovaný obsah. Spoločnosť dáta spárovala s IP adresou a predala marketingovým spoločnostiam. Súd okrem pokuty prikázal spoločnosti vymazať údaje zozbierané do 1.3.2016 a implementovať potrebu získať výslovný súhlas zákazníkov na zber dáta.

GovPayNow.com ponechala verejných 14 miliónov záznamov

14 miliónov záznamov za posledných 6 rokov mohlo uniknúť spoločnosti GovPayNet. V internetovej adrese ich webstránky bolo možné meniť číslo potvrdenky o platbe, a tak získať danú potvrdenku so všetkými údajmi na nej vystavenými. Spoločnosť poskytuje platobné služby asi 2300 vládnym agentúram v Spojených štátoch. Občania môžu cez portál GovPayNow.com hradiť poplatky a pokuty a dostanú online potvrdenie o zaplatení.

Únik 11 miliónov záznamov z marketingovej MongoDB databázy

Bezpečnostný výskumník objavil server s MongoDB databázou, patriaci kalifornskej marketingovej spoločnosti, ktorý obsahoval nezabezpečené osobné údaje 11 miliónov používateľov. Záznamy pozostávali z mien, e-mailových adries, pohlavia, miest, štátov a PSČ ich pobytu, ako aj DNS informácií a informácií o doručených e-mailoch. Navyše, v databáze bol nájdený záznam s názvom „Warning“, ktorý predstavoval informáciu o tom, že databáza unikla a neznámi útočníci vlastnia jej kópiu. Po zaplatení 0,4 bitcoinov ju údajne vymažú.

Pegasus, spyware pre platformy Android a iOS, nájdený v 45 krajinách

Správa zo spoločnosti Citizen Lab hovorí, že za posledné dva roky bolo zaznamenané rozšírenie spyware s názvom Pegasus pre mobilné zariadenia Android a iPhone do 45 krajín. Tento malvér infikuje zariadenia na diaľku a okrem iného umožňuje útočníkovi prístup k e-mailom, textovým správam, kalendáru, polohe, mikrofónu a kamere obete, bez jej vedomia. Vyvinula ho izraelská spoločnosť NSO Group, ktorá predáva podobné nástroje tajným službám a bezpečnostným zložkám po celom svete.

Krádež kreditných kariet zákazníkov Newegg

Útočníci z Magecart hacking group ukradli údaje o kreditných kartách zákazníkov Newegg, obchodníka s výpočtovou technikou a inou elektronikou. Na stránku Newegg sa im podarilo vložiť škodlivý JavaScript kód, ktorý odchytával platobné údaje a preposielal im ich. Únik postihol všetkých používateľov, ktorí zadali svoje platobné údaje medzi 14.8.-18.9.2018. Priemerná mesačná návštevnosť portálu je 50 miliónov používateľov.

Zanedbanie likvidácie dát po krachu spoločnosti NCIX viedlo k úniku dát zákazníkov, zozbieraných počas 15 rokov

Veľký kanadský obchodník s hardvérom, spoločnosť NCIX, nechala po krachu voľne dostupné citlivé údaje svojich zákazníkov a zamestnancov, ktoré zozbierala za posledných 15 rokov svojej existencie. Na stránku Craigslist sa tak dostala reklama na predaj hardvéru bývalej spoločnosti, na ktorom sa tieto citlivé údaje nachádzali. Výskumník Travis Doering sa pomocou nej dostal do skladu so stovkami počítačov a serverov patriacich spoločnosti NCIX, kde mu pracovníci dovolili odkúpiť a nakopírovať si obsah tam uložených pevných diskov. Nielen že spoločnosť NCIX nezlikvidovala po krachu citlivé údaje, ktoré by mohli byť zneužité, no ani len zálohy neboli šifrované. Doering tak našiel okrem iného osobné údaje zamestnancov a zákazníkov, faktúry, fotografie občianskych preukazov, telefónne čísla, IP adresy a heslá. Podarilo sa mu nájsť aj zálohu počítača zakladateľa spoločnosti NCIX, Steve Wu.

Online obchodu s oblečením SHEIN unikli údaje takmer 6 a pol milióna klientov

SHEIN

Spoločnosť SHEIN zaoberajúca sa predajom módneho oblečenia online utrpela v júni prienik do svojich systémov. O tejto skutočnosti sa dozvedela až koncom augusta a správu o ňom vydala o mesiac neskôr. Pri prieniku boli odcudzené citlivé údaje 6,42 milióna zákazníkov. Predstavovali používateľské e-mailové adresy a šifrované heslá.

Kybernetický útok na prístav v Barcelone

Koncom septembra sa odohral kybernetický útok na serveri Barcelonského prístavu. Zasiahnuté boli niektoré serveri a systémy. Spoločnosť spustila záložný plán vytvorený pre takúto situáciu. Útok neovplyvnil plavby lodí. Všetky námorné aj pozemné nákladné operácie fungovali štandardným spôsobom. Útok sa zhodou náhod odohral dva dni po tom, ako prístav zdieľal na svojom Twitteri článok o kybernetickej bezpečnosti so slovami, že nikto nie je pred kybernetickým útokom v bezpečí, dokonca ani prístavy.

Prienik do systémov Facebooku zasiahol 50 miliónov používateľov

Spoločnosť Facebook zverejnila koncom septembra informáciu o prieniku do svojich systémov. Útočníci údajne zneužili zraniteľnosť v kóde služby a ukradli prístupové tokeny používateľov, ktoré umožňujú zostať prihlásený vo svojom účte po zadaní mena a hesla. Došlo k tomu v momente, keď si používatelia prepli pohľad do „verejného profilu“ pomocou funkcie „View As“. Útočníci vďaka tokenom mohli prevziať kontrolu nad zasiahnutými používateľskými reláciami. Nie je zrejmé, či došlo k prístupu k používateľským dátam. Facebook postihnuté účty odhlásil a zresetoval im prihlasovacie tokeny.

Závažné zraniteľnosti bežných softvérových a hardvérových produktov

Tisíce MikroTik routerov zneužité na odpočúvanie komunikácie

Masívne odpočúvanie komunikácie cez MikroTik routery, ktoré bolo nedávno odhalené spoločnosťou 360 Netlab, bolo možné kvôli zraniteľnosti v nástroji Winbox v MikroTik RouterOS. Útočník jej zneužitím môže prevziať kontrolu nad routerom, odpočúvať sieťovú komunikáciu a vykonávať inú škodlivú činnosť.

Zraniteľnosť v Tor 7.x povoľuje spúšťanie JavaScript

Bol zverejnený exploit na zraniteľnosť v anonymizujúcom prehliadači Tor Browser. Zraniteľnosť sa nachádza v predinštalovanom prídavnom module NoScript vo verziách Tor Browser 7.x a umožňuje útočníkovi spúšťať ľubovoľný JavaScript kód. Možným zámerom môže byť odhalenie identity používateľa, resp. jeho IP adresy.

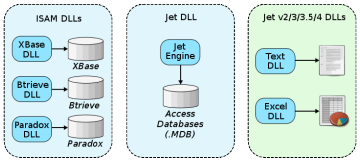
Cisco zraniteľnosti

Tento mesiac bolo objavených už 36 zraniteľností v produktoch spoločnosti Cisco, z čoho tri sú uvedené ako kritické.

Studeným štartom k informáciám zo šifrovaných diskov

Výskumníci z F-Secure odhalili spôsob ako znefunkčniť softvérovú ochranu pred útokom typu cold boot (studený štart) a získať tak citlivé dáta z pamäte RAM, okrem iného aj heslá a kryptografické kľúče k šifrovaným diskom. Zraniteľné sú takmer všetky dnešné osobné počítače a zatiaľ existujú len opatrenia na zníženie pravdepodobnosti úspešného útoku.

Kritická zraniteľnosť v Microsoft Jet Database Engine



V nástroji Microsoft Jet Database Engine existuje zraniteľnosť, ktorá spočíva v možnosti docieliť zápis do pamäte mimo povolených hodnôt. Po úspešnom zneužití môže útočník vzdialene vykonávať kód v kontexte aktuálneho procesu. V čase písania tohto článku neexistuje opravná aktualizácia.

Nárast počtu útokov na WordPress stránky

V súčasnosti bolo zaznamenané významné zvýšenie počtu kompromitácií WordPress webstránok. Útočníci napríklad upravili stránky tak, aby vybraných používateľov presmerovávali na podvodne služby technickej podpory. Jedným z vektorov útokov sú súbory installer.php vytvorené zraniteľnými verziami WordPress doplnku Duplicator. Útočníkom dovoľujú vzdialene vykonávať kód a prevziať kontrolu nad webserverom.

Peekaboo umožňuje ovládnuť bezpečnostné kamerové systémy

Kritická zraniteľnosť nazvaná Peekaboo bola odhalená v bezpečnostných monitorovacích systémoch spoločnosti NUUO. Chyba sa nachádza konkrétne v softvérovom riešení pre kamerový IP rekordér NVRMini2 pre CCTV/IP kamery. Po úspešnom zneužití môže útočník vzdialene spúšťať kód s administrátorskými privilégiami, sledovať a upravovať, či odpojiť živý signál z kamier a manipulovať s nahrávkami.

Zraniteľnosti Wireshark

Bolo opravených kritických 6 zraniteľností produktu Wireshark, verzií 2.2, 2.4 a 2.6, vedúcich k Denial of Service podmienkam. Konkrétne sa jedná o zraniteľnosti CVE-2018-14340, CVE-2018-14344, CVE-2018-14367, CVE-2018-14368, CVE-2018-14369, CVE-2018-14370.

Zraniteľnosti Oracle WebCenter Interaction

ORACLE
WebCenter

Niekoľko závažných zraniteľností bolo opravených v produkte Oracle WebCenter Interaction 10.3.3 (a pravdepodobne starších). Útočníkom umožňujú vykonať útoky typu XSS, CSRF, DoS. Môže dôjsť k úniku informácií, ako napríklad dáta z profilov používateľov. Útočníci môžu spúšťať ľubovoľný kód v prehliadači v rámci zasiahnutej domény, získať zvýšené privilégiá, či vykonávať phishingové útoky.

Mesačník zraniteľností September 2018

CSIRT.SK vydáva a uverejňuje na svojej stránke prehľad kritických zraniteľností bežného softvérového vybavenia na mesačnej báze. Jedná sa o nasledovné produkty:

1. Operačné systémy Microsoft Windows
2. Kancelárske balíky Microsoft Office a Office Web Apps
3. Internetové prehliadače
    - Microsoft Internet Explorer
    - Microsoft Edge
    - Mozilla Firefox
    - Google Chrome
4. Adobe Flash Player
5. Frameworky
    - Microsoft .NET Framework
    - Oracle
6. Iné tohtomesačné závažné zraniteľnosti
    - Peekaboo
    - Útoky na WordPress stránky
    - Microsoft Jet Database Engine
    - Znefunkčnenie ochrany proti cold boot útoku
    - Cisco zraniteľnosti
    - Tor 7.x zraniteľnosť
    - MikroTik routery - zraniteľnosť

https://www.csirt.gov.sk/aktualne-7d7.html?id=162

TLP: White