Trusteos SRL
București, str. Ion Nistor nr. 4
0727 077 111, info@trusteos.ro

Nr. 32 din 3 iulie 2020

INFORMARE PERIODICĂ

PRIVIND

PROTECȚIA DATELOR CU CARACTER PERSONAL

Conform cerințelor

Regulamentului UE 679/2016 (GDPR)

Informații și recomandări pentru protecția datelor

Notă introductivă

Prin păstrarea caracterului actual și prin acuratețea informației disponibile, cu relevanță pentru protecția datelor cu caracter personal, este îmbunătățită capacitatea de apărare față de eventuale amenințări cibernetice și se reduce impactul eventualelor riscuri concretizate în situațiile inevitabile.

Informarea periodică are menirea de a contribui la pregătirea persoanelor implicate în activități de prelucrare a datelor cu caracter personal, astfel încât să poată combate eficient atacurile și încercările neautorizate de acces la informații protejate, prin identificarea și blocarea operativă a acestora.

Sursele selectate pentru culegerea informațiilor au reputație excelentă, de specialitate, cu caracter oficial, implicate în efortul comun internațional pentru protecția datelor, inclusiv prin organizații, asociații, instituții și autorități de profil. Exemplele prezentate servesc ca modele de urmat, în cazul recomandărilor, sau de evitat, în cazul materializării unor riscuri, ca urmare a neglijării unor vulnerabilități ale infrastructurii IT.

Noutăți din domeniul protecției datelor

i. Swiss Re atrage atenția asupra nevoii de transparență în privința atacurilor cibernetice

Producerea rapoartelor referitoare la atacurile cibernetice materializate contribuie la întărirea capacității de rezistență față de astfel de amenințări ulterioare. Unele tipuri de atacuri s-au înmulțit considerabil, îndeosebi în contextul muncii de la distanță, cum ar fi creșterea trimestrială cu 25% a amenințărilor de tip **ransomware**.

Conform Financial Times, astfel de rapoarte privind atacurile cibernetice pot descrie măsurile tehnice și organizatorice de protecție a datelor, aplicarea acestora în practică și remediile utilizate în scopul îmbunătățirii securității cibernetice, inclusiv prin asigurarea riscurilor, care va crește cu 22% în acest an.

ii. Australia a înregistrat atacuri cibernetice masive pentru exploatarea de criptomonede

Centrul de securitate cibernetică din Australia a anunțat că un grup de atacatori cibernetici au accesat ilegal rețele informatice pentru a exploata vulnerabilitățile sistemelor informatice în scopul furtului de criptomonedă, utilizând malware.

Patru astfel de vulnerabilități critice ale interfeței Telerik UI, cum ar fi CVE 2019-18935, au fost exploatate de grupul Blue Mockingbird pentru a instala pe mii de sisteme informatice softul de minare de criptomonedă Monero XMRRig.

Unele programe malware identificate, ca PlugX, au fost asociate cu atacatori din China, existând inclusiv suspiciuni privind susținerea acestora de organizații statale, conform CoinTelegraph.

iii. Atacatorii utilizează fișiere de tip .slk pentru infiltrarea în conturile clienților Microsoft 365

Hackerii au utilizat o nouă metodă de atac, care ocolește atât sistemul implicit de securitate Microsoft 365 EOP, cât și modulul avansat de securitate ATP.

Fișierele de tip .slk includ comenzi macro, care descarcă și instalează un troian pentru acces de la distanță, conform experților în securitate cibernetică de la Avanan.

Atacurile au fost destul de rare și foarte bine țintite, fiind derulate prin emailuri cu un grad ridicat de personalizare și relevanță pentru persoana și organizația vizată.

Mesajele au fost trimise de pe mii de adrese hotmail, conținutul fiind caracterizat de caractere speciale incluse în text cu scopul de a deruta sistemele de detecție și blocare, divizând comanda macro în două secțiuni, conform celor de la GBHackers.

iv. Hackerii ascund cod malițios în imagini pentru a citi datele de pe carduri bancare

Dacă prezența fizică a cititoarelor frauduloase de carduri este relativ ușor de identificat pe ATM-uri, este mult mai dificilă sesizarea acestora online, în coșurile de cumpărături și modulele utilizate pentru plăți virtuale.

Chiar dacă ascunderea de malware în codul JavaScript după imagini (favicons) este o metodă cunoscută de fraudă, este o premieră ascunderea în acest mod a unor cititoare frauduloase a datelor de pe cardurile bancare.

Conform celor de la **Engadget**, astfel de atacuri s-au derulat prin extensia WooCommerce pentru WordPress, cu o utilizare foarte răspândită la nivel internațional, ceea ce face din ea o țintă atractivă pentru atacatori.

v. Compartimentul de taxe și impozite din Polk, Florida a fost ținta unui atac cibernetic

Un oraș din statul american Florida a anunțat că sistemele informatice ale compartimentului de taxe și impozite au fost blocate două zile, în urma unui atac cibernetic.

Atacul a începul cu un email care părea să conțină o factură, fiind de fapt un fișier infectat cu un virus informatic. Măsurile de protecție au detectat atacul și au limitat răspândirea și impactul asupra celorlalte sisteme informatice din rețeaua locală, fără să fie compromise datele cu caracter personal ale contribuabililor.

Conform **The Ledger**, funcționarea a fost supendată ca măsură de precauție pentru toate dispozitivele electronice compartimentului, inclusiv telefoanele, până la curățarea și

testarea acestora, proceduri care se estimează că vor dura o săptămână.

vi. Activități suspecte: 54 de aplicații iOS și 47 de aplicații deghizate ca jocuri pentru Android

Cele 54 de aplicații populare iOS citesc text din datele conținute în fișierele utilizatorilor fără o justificare temeinică, inclusiv TikTok, conform experților în securitate cibernetică citați de Ars Technica.

Astfel de texte pot include parole, adrese ale portofelelor de criptomonedă, mesaje personale și orice alte informații stocate astfel pe dispozitivele iOS.

Acest comportament periculos se poate extinde și la dispozitive apropiate, care utilizează temporar aceleași ID-uri Apple:

ABC News	My Emma
Al Jazeera English	Plants vs. Zombies™ Heroes
CBC News	Pooking – Billiards City
CBS News	PUBG Mobile
CNBC	Tomb of the Mask
Fox News	Tomb of the Mask: Color
News Break	Total Party Kill
New York Times	Watermarbling
NPR	TikTok
ntv Nachrichten	ToTalk
Reuters	Tok
Russia Today	Truecaller
Stern Nachrichten	Viber
The Economist	Weibo
The Huffington Post	Zoosk
The Wall Street Journal	10% Happier: Meditation
Vice News	5-0 Radio PoliceScanner
8 Ball Pool™	Accuweather
AMAZE!!!	AliExpress Shopping App
Bejeweled	Bed Bath & Beyond
Block Puzzle	Dazn
Classic Bejeweled	Hotels.com

Classic Bejeweled HD	Hotel Tonight
FlipTheGun	Overstock
Fruit Ninja	Pigment – Adult Coloring Book
Golfmasters	Recolor Coloring Book to Color
Letter Soup	Sky Ticket
Love Nikki	The Weather Network

De asemenea, dispozitivele Android pot fi infectate de 47 de jocuri cu comportamente ascunse, malițioase și de tip Adware. Acestea au fost descărcate de peste 15 milioane de ori, conținând deseori viruși troieni, capabili să execute comenzi fără acceptul utilizatorului.

Multe dintre acestea își ascund prezența după instalare, făcând mai dificilă înlăturarea lor, conform experților de la Avast, citați de **TechRadar**:

Draw Color by Number	Throw Master
Skate Board – New	Throw into Space
Find Hidden Differences	Divide it – Cut & Slice Game
Shoot Master	Tony Shoot – NEW
Stacking Guys	Assassin Legend
Disc Go!	Flip King
Spot Hidden Differences	Save Your Boy
Dancing Run – Color Ball Run	Assassin Hunter 2020
Find 5 Differences	Stealing Run
Joy Woodworker	Fly Skater 2020

vii. Google a dezafectat alte 25 de aplicații Android care fură datele de logare pe platforma Facebook

Experții de la **ZDNet** anunță că Google a constatat în ultima lună activități frauduloase ale unui număr de aplicații Android descărcate în total de peste 2,34 de milioane de ori.

Aplicațiile au fost scoase din lista Google Play și indisponibilizate, promițând diferite facilități pentru utilizatori și având funcționalități comune, semn că au fost dezvoltate de același grup infracțional.

Se recomandă ca utilizatorii care le au pe dispozitive să le înlăture imediat și să-și schimbe parolele de acces pe care le folosesc în prezent pentru contul de Facebook:

Super Wallpapers Flashlight	Junk file cleaning
Padenatef	Synthetic Z
Wallpaper Level	File Manager
Countour level wallpaper	Composite Z
iPlayer&iWallpaper	Screenshot Capture
Video Maker	Daily Horoscope Wallpapers
Color Wallpapers	Wuxia Reader
Pedometer	Plus Weather
Powerful Flashlight	Anime Live Wallpaper
Super Bright Flashlight	iHealth Step Counter
Solitaire Game	TQY Fiction
Accurate scanning of QR code	Classic card game

viii. Se răspândesc aplicații frauduloase care pretind că reprezintă serviciile poștale ale unor țări

Programul malware denumit FakeSpy este capabil să transmită mesaje text malițioase, să spioneze datele personale de pe dispozitivele pe care le infectează și să preia controlul asupra lor, folosind o tehnică identificată ca SMS phishing.

Pentru a-și camufla intențiile, mesajul pretinde că provine de la expeditori cunoscuți, cum ar fi serviciile poștale din SUA, Franța, Germania, Marea Britanie, Japonia, Taiwan și Elveția, redirecționând utilizatorii către website-uri care par legitime.

Experții de la Cybereason citați de **TomsGuide** recomandă evitarea acțiunilor solicitate prin SMS-uri neașteptate, cum ar fi deschiderea linkurilor, descărcarea unor aplicații și instalarea lor.

ix. Bazele de date aparținând unor companii au fost puse la vânzare online, pe piața neagră

Un broker de date informatice a pus în vânzare baze de date cu înregistrări aferente utilizatorilor obținute prin breșe de securitate de la 14 companii.

Compania	# de înregistrări	Data breșei
DarkThrone	282,825	iunie 2020
Efun	2.2 milioane	2020
Fluke	353,321	iunie 2020
Footters	209,783	iunie 2020
HomeChef	8 milioane	2020
JamesDelivery	1.6 milioane	martie 2020
KitchHike	115,480	iunie 2020
KreditPlus	896,170	iunie 2020
Minted	4.3 milioane	mai 2020
Playwings	4.1 milioane	aprilie 2020
Revelo	1.1 milioane	iunie 2020
Tokopedia	91 milioane	aprilie 2020
Yotepresto	1.4 milioane	iunie 2020
Zoosk	29.1 milioane	ianuarie 2020

Combinate, aceste baze de date totalizează peste 132 de milioane de înregistrări aparținând utilizatorilor, care pot fi utilizate în atacuri disimulate asupra altor ținte.

Experții de la **Bleeping Computer** spun că brokerul oferă spre vânzare și informații provenind din breșe mai vechi, incluzând Star Tribune, EpicGames, ZyngaPoker, ReverbNation, Wirecard, ClickFunnels și multe altele, ceea ce contribuie la creșterea nivelului de alertă.

x. Microsoft a publicat remedii pentru două vulnerabilități aferente Windows 10

Identificate ca CVE-2020-1425 și CVE-2020-1457, prima este considerată critică, iar cea de-a doua importantă ca severitate, fiind afectate atât serverele, cât și desktop-urile.

Acestea permiteau atacatorilor să exploateze sistemele informatice în scopul executării arbitrare de cod și să compromită rețelele aferente. Remediile au fost incluse într-o actualizare automată, conform experților de la TrendMicro.

xi. Companii uriașe au fost afectate de atacurile ransomware Maze

LG și Xerox au fost adăugate pe lista victimelor infractorilor cibernetici, care au reușit să acceseze domenii și sisteme informatice ale acestora, criptând ilicit datele.

Atacatorii au publicat online detalii despre furtul a peste 100GB de date cuprinse în fișierele criptate, cu capturi de ecran care să le susțină afirmațiile, solicitând o recompensă considerabilă în schimbul restabilirii accesului la informații.

xii. Un program malware camuflat foarte bine a fost recent detectat de experții Sophos

Denumit Glupteba, programul utilizează o multitudine de tehnici creative specifice malware pentru disimulare, inclusiv prin invadarea modulelor de detecție Windows Defender printre excepții, mascând comunicările și instalând comenzi pentru

De asemenea, include instrumente de monitorizare a proceselor, reducând șansele de detectare și declanșare a unei alerte în sistem.

Acest program culege informații inclusiv din browser, instalează programe de minare de criptomonedă, consumând energia sistemului infectat și arzându-i procesorul mai repede, conform celor de la **TechRadar**.

Acțiuni ale autorităților

1. Încălcarea regulilor de protecție a datelor personale aparținând minorilor a fost sancționată cu 100,000 de dolari

O platformă social media „We Heart It" dedicată copiilor a încălcat regulile privind protecția datelor personale ale acestora, permițând înscrierea membrilor minori fără acordul parental obligatoriu. De asemenea, a colectat datele acestora și a permis accesul unor companii care le-au utilizat în scopuri publicitare.

Super Basic LLc și Maple Media LLc vor avea de plătit încă 400,000 de dolari, dacă întârzie să efectueze modificările impuse de lege pentru cei aproximativ 500,000 de utilizatori activi săptămânal.

Aceștia distribuie imagini și alte tipuri de conținut, comunică și interacționează pe canalele dedicate unor teme atractive pentru copii, ca Disney, Harry Potter, Pokemon sau celebrități ca Taylor Swift și Ariana Grande, fără ca platforma să facă o verificare elementară a vârstei la momentul înscrierii.

Companiile au obligația de a utiliza un filtru, pentru a împiedica înscrierea în platforma social media pentru utilizatori care nu au împlinit 13 ani. De asemenea, vor solicita obligatoriu un acord parental verificabil, înainte de colectarea datelor personale de la copii sub 13 ani și vor informa direct părinții în privința politicii de prelucrare a datelor colectate.

Totodată, în termen de 15 luni, companiile vor avea obligația de a finaliza examinarea tuturor conturilor de utilizatori și vor elimina orice conturi care le aparțin unor minori, conform **iapp.org**.

2. Autoritatea din Danemarca a sancționat municipalitatea Lejre cu o amendă de 50,000 de coroane

Încălcarea prevederilor GDPR sancționată a constat în neîndeplinirea obligațiilor ce revin unui operator de date cu

caracter personal privind protecția acestora, prin publicarea pe propriul portal a unor informații referitoare la cetățeni.

Un număr mare de angajați ai municipalității au avut acces la aceste informații, care includeau și referiri la minori, sub vârsta de 18 ani. Acest lucru a devenit cunoscut autorității în urma raportării unui incident de securitate, care nu a fost adus însă și la cunoștința persoanelor vizate.

3. Autoritatea de protecție a datelor personale din landul Baden-Wurttemberg a aplicat o amendă de 1.24 milioane de Euro

Sancțiunea a fost dictată împotriva unei companii de asigurări de sănătate, AOK. Aceasta a organizat tombole și concursuri cu utilizarea datelor personale ale asiguraților în scopuri publicitare, fără implementarea măsurilor necesare acestor activități.

Datele aparținând unui număr de aproximativ 500 de persoane au fost prelucrate în acest mod, fără consimțământul lor expres, între 2015 și 2019.

4. Autoritatea din Franța a emis noi recomandări pentru politica de cookies și evaluările de impact (DPIA)

CNIL a publicat o nouă versiune a softului dedicat evaluării de impact (DPIA) pentru a facilita managementul analizelor privind activitățile de prelucrare de date cu caracter personal.

Instrumentul este disponibil și poate fi descărcat inclusiv în limba română. Programul permite căutarea după cuvinte cheie, filtrarea, corecturile, categorizarea informațiilor, mangementul versiunilor evaluării și arhivarea analizelor.