Udhëzues për përdoruesit rreth incidenteve të sigurisë

Adresa: Rruga Hoxha Tahsin, Nd. 113, H. 1, Njësia Administrative Nr. 2, 1017
Mail: contact@softsolution.al, Website: www.softsolution.al
Tel: +355 67 600 66 33

Për të mbrojtur klientët e saj dhe në zbatim të Rregullores Nr.37 datë 29.10.2015 "MBI MASAT TEKNIKE DHE ORGANIZATIVE PER TE GARANTUAR SIGURINE DHE INTEGRITETIN E RRJETEVE DHE/OSE SHERBIMEVE TE KOMUNIKIMEVE ELEKTRONIKE", kompania "Soft & Solution", publikon këtë udhëzues për përdoruesit "**Rreth incidenteve më të zakonshme të sigurisë, veprimeve dhe/ose mjeteve që duhen ndjekur për të parandaluar ndodhjen e këtyre incidenteve dhe veprimeve që duhen ndjekur pas ndodhjes së incidenteve të sigurisë**"

Me qëllim mbrojtjen tuaj nga aktivitete me natyrë mashtruese në fushën e komunikimeve elektronike, Soft & Solution dëshiron t'ju japë disa këshilla të thjeshta.
Jeni të lutur të mos ju përgjigjeni email-ve mashtruese që ju bëjnë me dije se jeni fitues i një llotarie apo një çmimi të caktuar kur në të vërtetë ju nuk keni marrë pjesë në asnjë lojë apo shorte që të mundësojë një gjë të tillë. Zakonisht këto email-e apo telefonata kryhen në mënyrë automatike nga platforma kompjuterike të paidentifikuara jashtë vendit. Shpesh herë nëse ju dërgoni e-mail apo kryeni thirrje drejt këtyre numrave mund të jeni subjekt i tarifave premium të padëshiruara. Prandaj, shmangni kryerjen e thirrjeve drejt numrave ndërkombëtare të panjohur.

Soft & Solution angazhohet të mbrojë klientet e saj duke u komunikuar si të sillen ne raste te tilla.
Ju lutemi, mos telefononi numra ndërkombëtarë të cilët nuk i njihni sepse këta numra mund të rezultojnë me tarifa tepër të larta.

Përdorimi i kujdesshëm i rrjeteve sociale

Menaxhoni privatësinë në rrjetet sociale duke zgjedhur se cilët mund te shohin profilin tuaj.Kontrolloni postimet që ju bëni. Mos publikoni foto të fëmijëve tuaj të cilat japin informacion mbi vendndodhjen e tyre. Përzgjidhni me kujdes personat që zgjidhni të bëni miq dhe bllokoni hyrjet e padëshiruara.

Kujdes kur lidheni me wireless-a që janë pa password

Mos vendosni të dhënat tuaja personale dhe passwordet tuaja kur lidheni me wireless që janë pa password pasi faqet mund të duken sikur janë njësoj por mund të marin të dhënat tuaja personale. Ju këshillojmë që te përdorni programe VPN .

Çfarë është Hackimi?

Aksesimi i të dhënave në një sistem kompjuterik në mënyrë të pa autorizuar dhe pa pasur miratimin e personit përgjegjës për këtë rrjet, për të përdorur të dhënat sipas interesave vetjake.

Mbrojtja nga hackimi i mundshëm i pajisjeve në rrjet:

Krijimi i akses listave (ACL) për të bllokuar çdo IP të jashtme (jo Soft & Solution) për të pasur mundësi aksesi tek pajisja.

Bllokimi i komunikimeve në portën 20 & 21 (FTP), 22 (SSH), 23 (telnet).

Aksesi lejohet për klientët të cilët i përdorin këto porta

Vendosja e password-eve në mënyrë të personalizuar për çdo klient. Password-et sugjerohet të jenë të përbërë nga: (minimalisht 1 për çdo kategori)

- Shkronja (të vogla & kapitale)
- Numra (0-9)
- Karaktere special (psh. @#$%^&)

Aktivizimi i firewall si në PC dhe në router për të eliminuar ndërhyrjet e pa autorizuara në rrjet.

Instalimi i antivirusit në kompjuter për të qenë i mbrojtur nga infektimit i tij.

Meltdown dhe Specter

Meltdown dhe Specter janë dy prej të metave të zbuluara kohët e fundit në proçesorët që përdorin shumica e pajisjeve elektronike duke ekspozuar dhe vënë në rrezik të dhënat që ruhen në memoriet e brendshme të këtyre pasijeve.

SOFT & SOLUTION, ju sugjeron hapat e mëposhtme teknike në mënyre që të mbroni pajisjen tuaj nga këto probleme.

Çfare janë Specter dhe Meltdown?

Specter dhe Meltdown janë emrat e të metave të zbuluara në një numër proçesorësh nga Intel, ARM dhe AMD, duke shfrytëzuar këto te meta hakerat mund të kenë qasje në fjalëkalime, çelësa inkriptimi dhe informacione të tjera private nga aplikacionet e hapura.

Këto të meta janë zbuluar nga një numër i madh institutesh kërkimore dhe rezultatet po dërgojnë valë tronditëse informacioni nëpër botën e Teknologjisë së Informacionit. Në të vërtetë, u zbulua se këto probleme kane qenë prezente në dizajnin e çipeve për më shumë se 20 vjet dhe se ato afektonin një numër shume të madh procesorësh të integruara në pajisje te ndryshme elektronike nga PC-të në servera dhe madje edhe smartphone-s .

Adresa: Rruga Hoxha Tahsin, Nd. 113, H. 1, Njësia Administrative Nr. 2, 1017
Mail: contact@softsolution.al, Website: www.softsolution.al
Tel: +355 67 600 66 33

A duhet të shqetësohem për Specter dhe Meltdown?

Për momentin, ju nuk duhet të panikoni shumë, sepse deri më tani nuk duket nëse të metat e Specter ose Meltdown janë përdorur në ndonje sulm kibernetik dhe prodhuesit e këtyre pajisjeve po punojnë me Intel, ARM dhe AMD për të rregulluar këto defekte.
Intel ka pohuar se shfrytëzimet nuk mund të korruptojnë, modifikojnë ose fshijnë të dhënat dhe jane duke punuar për të gjetur zgjidhje për këto të meta duke konsideruar dhe redesign të proçesoreve.

Pra, mos u shqetësoni shumë, por mbani një sy në çdo përditësim të pajisjes suaj dhe ndiqni këshillat tona se si të mbroheni nga gabimet e sigurisë së CPU të Meltdown dhe Specter.

Si të mbrohemi nga të metat e sigurisë Meltdown dhe Specter

Më poshtë do të gjeni mënyra për të rregulluar dhe mbrojtur veten kundër te metave të sigurisë së Meltdown dhe Specter për një sërë pajisjesh.

Apple Update: Apple ka lëshuar përditësimin e iOS 13 dhe përditësimin MacOS 10.14.6 për të ndihmuar në zvogëlimin e të metave të Meltdown dhe Specter.

Si të rregulloni gabimet e sigurisë Meltdown dhe Specter në telefonat Android

Google do lëshoi një përditësim të ri të sigurisë më 5 janar 2018 i cili do ndihmoi në mbrojtjen e Android telefonit tuaj kundër Meltdown dhe Specter.

Si të rregulloni të metat e sigurisë Meltdown dhe Specter në Windows PC

PC-të e Windows-it ka gjasa që të goditen më së shumti nga Meltdown dhe Specter, pavarësisht nëse ato zhvillohen në procesorë Intel ose AMD. Lajm i mirë është se Microsoft konfirmon se ka lëshuar tashmë një update të sigurisë të për Windows 10, si dhe versionet e mëparshme të Windows.

Në Windows 10 përditësimet bëhen automatikisht, për të qenë të sigurtë, shtypni "dritaret e përditësimit" në shiritin e kërkimit të taskbar dhe zgjidhni "Kontrollo për përditësime".

Shkarkoni dhe instaloni çdo përditësim të ri që gjeni.

Si të rregulloni të metat e sigurisë Meltdown dhe Specter në Mac

Dhe pajisjet Mac-s gjithashtu janë prekur nga Meltdown dhe Specter. Apple gjithashtu ka shtuar se tashmë ka lëshuar një sërë rregullimesh në MacOS 10.14.6, për çdo përditësim të OS X ose macOS dhe sigurohuni që ju keni versionin e fundit të sistemit operativ.

Adresa: Rruga Hoxha Tahsin, Nd. 113, H. 1, Njësia Administrative Nr. 2, 1017
Mail: contact@softsolution.al, Website: www.softsolution.al
Tel: +355 67 600 66 33