P4I (Digital360): cosa fare per proteggersi dalle falle dei processori

Installare tutti gli aggiornamenti dei dispositivi, aggiornare il browser e utilizzare filtri per la navigazione come gli AdBlocker. Assicurarsi anche che i fornitori di servizio si stiano occupando del problema.

Condividere le informazioni sul problema ai propri contatti attraverso un messaggio breve e chiaro con i rimandi ai siti ufficiali.

Milano, 8 gennaio 2018 - Installare tutti gli aggiornamenti dei dispositivi, aggiornare il browser, utilizzare filtri per la navigazione, come gli AdBlocker, e assicurarsi che tutti i fornitori di servizio si stiano occupando del problema. Sono questi, in sintesi, i consigli degli esperti di **P4I – Partners4Innovation**, società del Gruppo **Digital360**, per proteggere i dispositivi da "Meltdown" e "Spectre", le due gravi vulnerabilità emerse negli scorsi giorni, frutto di un errore di progettazione presente dal 1995, che rende attaccabili i processori di quasi tutti i dispositivi utilizzati quotidianamente (server, server cloud, PC Windows e Linux, MAC, smartphone, tablet, etc.), da cui possono essere sottratte informazioni critiche e riservate. In questi giorni saranno pubblicati ulteriori dettagli su queste vulnerabilità, mentre i diversi produttori stanno rilasciando gli aggiornamenti necessari per correggere il problema, che purtroppo rallenteranno i dispositivi in modo sensibile. Il sito di riferimento per restare aggiornati in tempo reale sul tema è https://meltdownattack.com.

Come difendersi – Per proteggersi dalle falle dei processori però, spiega P4I, innanzitutto è necessario verificare che tutti gli aggiornamenti di sistema proposti siano applicati, sia sul computer che su altri device, come telefoni, tablet ecc. Poi, bisogna assicurarsi che tutti i browser utilizzati siano aggiornati. E verificare di utilizzare un AdBlocker, uno di quei componenti aggiuntivi dei browser che impediscono che sulle pagine visitate vengano visualizzate pubblicità e che il dispositivo esegua script, perché questo potrebbe essere uno dei principali vettori di attacco da parte dei criminali. "Vista la grande attenzione che il tema sta suscitando presso il grande pubblico – avverte **Gabriele Faggioli**, CEO di P4I e responsabile scientifico dell'Osservatorio Information Security & Privacy del Politecnico di Milano – non si esclude che a breve diversi siti malevoli propongano aggiornamenti, capaci di diventare il vettore dell'attacco: bisogna sempre porre grande attenzione ai siti visitati, installando aggiornamenti solo da fonti ufficiali".

In ambito aziendale è opportuno utilizzare le procedure di Patch Management per testare gli aggiornamenti pubblicati dai diversi vendor, per assicurarsi che non creino problemi, ed eseguirne il corretto deployment su tutti i dispositivi aziendali interessati. E' inoltre opportuno assicurarsi che i propri fornitori di servizio (Cloud, IaaS o SaaS) si stiano occupando nel modo corretto del problema.

Cosa si è scoperto - Alcuni ricercatori di Google hanno pubblicato un documento nel quale spiegano per la prima volta il problema: https://googleprojectzero.blogspot.it/2018/01/reading-privileged-memory-with-side.html. L'errore di progettazione scoperto permette ad un programma malevolo, creato appositamente, di eseguire sul dispositivo attaccato operazioni non autorizzate, non volute, che possono portare al furto di informazioni, dalle password alle chiavi crittografiche. Nel caso in cui si sia stati vittima dell'attacco è quasi impossibile scoprirlo.

La vulnerabilità – spiegano gli esperti di P4I – sfrutta le cosiddette "speculazioni" dei moderni processori, cioè funzionalità che permettono di velocizzare l'esecuzione dei programmi per precalcolare informazioni, in modo da avere risultati "già elaborati" quando necessario. L'errore nel disegno di queste funzionalità può permettere ad un programma malevolo, eseguito sul dispositivo attaccato, di "evadere" la normale segregazione tra applicazioni. "Su un dispositivo personale questo significa poter leggere i dati in RAM di altre applicazioni – spiega **Alessio L.R. Pennasilico**, Information & Cyber Security Advisor di P4I e Presidente di AIP, Associazione Informatici Professionisti –. In ambiente enterprise, di leggere i dati di altre istanze da una virtuale, si pensi ad infrastrutture Citrix, XEN, CMWare, AWS, Azure, etc".

Meltdown, catalogato come CVE-2017-5754, affligge solo i processori Intel. È il più semplice da sfruttare ed anche il più semplice da rimediare, per il quale sono già disponibili le patch da parte di diversi produttori. Qui è disponibile, aggiornato in tempo reale, l'elenco degli aggiornamenti disponibili: https://github.com/hannob/meltdownspectre-patches.

Spectre, meglio descritto nel paper https://spectreattack.com/spectre.pdf, catalogato in due varianti con CVE-2017-5753 e CVE-2017-5715, affligge i processori Intel, AMD ed ARM. Più difficile da utilizzare, è anche il grave e più difficile da correggere. Probabilmente ne discuteremo e ne subiremo le conseguenze ancora a lungo.

Gli aggiornamenti di fatto disabilitano la funzione che permette di "predire" le prossime operazioni, causando rallentamenti fino al 20 / 30% dell'hardware posseduto. Si consiglia in proposito la lettura dell'articolo https://access.redhat.com/articles/3307751.

Come essere utili? È utile fare informazione sul problema. "Ad esempio, utilizzare i canali account Social per pubblicizzare la questione tra i conoscenti – dice Gabriele Faggioli, CEO di P4I e responsabile scientifico dell'Osservatorio Information Security & Privacy del Politecnico di Milano –. Vista la complessità degli aspetti tecnici, è consigliabile un messaggio breve e chiaro, contenente i rimandi ai siti ufficiali". Un esempio: *"A causa di un errore di progettazione di molti processori, quasi tutti i nostri strumenti elettronici sono attaccabili e possono essere sottratte informazioni critiche e molto riservate che ci riguardano. Installa tutti gli aggiornamenti che ti vengono proposte dai dispositivi, aggiorna il browser. Utilizza filtri per la navigazione, come gli AdBlocker. Assicurati che i tuoi fornitori di servizio si stiano occupando del problema*".

Digital360

Digital360 si pone l'obiettivo di accompagnare imprese e pubbliche amministrazioni nella comprensione e nell'attuazione della trasformazione digitale e favorirne l'incontro con i migliori fornitori tecnologici. Digital360 persegue questo obiettivo attraverso una piattaforma multicanale unica in Italia – definita "MatchMaking Platform" - composta da portali online, white paper, eventi, webinar, servizi di comunicazione e marketing, lead generation e advisory. Digital360 integra un mix multidisciplinare e multiculturale di professionalità e competenze grazie ad analisti, giornalisti, consulenti ed esperti del mondo digitale, accumunati da una grande passione e missione: l'innovazione digitale come motore della crescita e dell'ammodernamento del nostro Paese. Per altre informazioni: www.digital360.it

Ufficio stampa Digital360: d'I comunicazione

Piero Orlando po@dicomunicazione.it mobile +39 3351753472