OUCH! | Iunie 2017

Buletinul informativ lunar de sensibilizare asupra securității pentru utilizatorii de calculatoare

OUCH!

În această ediție…

- Generalități
- Actualizarea
- Copii de siguranță
- Atacurile de Phishing

Învățăminte de pe urma WannaCry

Generalități

Recent, e foarte probabil să fi văzut nenumărate știri despre noul atac cibernetic numit „WannaCry”. „WannaCry” a infectat mai mult de 200000 de calculatoare, blocând accesul la datele proprii pentru o mulțime de organizații, inclusiv spitale din Marea Britanie. Există mai multe motive pentru care acest atac a atras atenția în mod deosebit. În primul rând, s-a propagat rapid de la un calculator la altul exploatând o vulnerabilitate cunoscută a sistemelor de operare Windows. În al doilea rând, atacul a fost din categoria „Ransomware”, ce înseamnă că odată ce a infectat calculatorul a criptat toate fișierele, blocându-vă accesul la propriile date. Singurul mod în care vă puteți recupera datele este să apelați la copiile de siguranță sau plătind atacatorului o răscumpărare de 300 de dolari pentru decriptarea datelor personale. În al treilea rând și cel mai important, acest atac nu ar trebuit să se întâmple. Vulnerabilitatea exploatată de „WannaCry” pe calculatoarele cu Windows a fost bine-cunoscută pentru Microsoft, care au publicat o actualizare menită să o rezolve cu luni în urmă. Însă multe organizații nu au reușit să instaleze această actualizare sau încă folosesc sisteme precum Windows XP, care sunt atât de vechi încât nu mai există actualizări disponibile. Iată trei pași simpli pe care-i puteți parcurge pentru a vă asigura că atacuri precum „WannaCry” nu vă vor afecta vreodată.

Editor Invitat

Dr. Johannes Ullrich este decanul cercetării la institutul SANS și fondatorul DShield.org. Este responsabilul Centrului de monitorizare și alertă **SANS Internet Storm Center**, care urmărește amenințările de securitate cibernetică curente. Predă Securitatea Aplicațiilor Web (**DEV522**), Detecția Intruziunilor (**SEC503**) și despre protocolul IPv6 (**SEC546**).

Actualizarea

În primul rând și înainte de toate, asigurați-vă că toate calculatoarele, dispozitivele mobile, aplicațiile și orice altceva conectat la Internet sunt actualizate. Răufăcătorii caută în permanență noi vulnerabilități în programele dispozitivelor pe care le folosiți. Atunci când descoperă astfel de vulnerabilități, folosesc programe speciale pentru a accede la sistemele pe care le folosiți. În acest răstimp, companiile care au dezvoltat programele folosite de dumneavoastră muncesc din greu pentru rezolvarea acelor vulnerabilități publicând noi versiuni actualizate ale programelor. Asigurându-vă că dispozitivele mobile și calculatoarele personale au instalate aceste actualizări, veți face mult mai dificil accesul răufăcătorilor la ele. Aceasta face cazul propagării „WannaCry” cu-atât mai frustrant. Actualizarea menită să rezolve și să stopeze acest atac a fost publicată de Microsoft încă de-acum două luni. Dacă organizațiile și-ar fi actualizat calculatoarele, acest atac nu ar fi avut succes. Pentru a fi siguri că dispozitivele personale sunt la zi, activați opțiunea de actualizare automată a acestora ori de câte ori e posibil. Această regulă se aplică aproape oricărui tip de tehnologie conectată la o rețea, nu numai calculatoarelor

Învățăminte de pe urma WannaCry

și dispozitivelor mobile, dar și televizoarelor conectate la Internet, echipamentelor de rețea domestice, consolelor de jocuri și, într-o bună zi, probabil că și propriului autoturism. Dacă sistemul de operare sau dispozitivele folosite sunt atât de vechi încât nu mai beneficiază de actualizări de securitate, cum e, bunăoară, Windows XP, înlocuiți-le cu unele noi, care au suportul furnizorului.

Cheia în protecția față de atacuri precum „WannaCry" stă în trei pași simpli: păstrați-vă calculatoarele actualizate, fiți precauți față de atacurile de Phishing și faceți copii de siguranță a sistemelor.

Copii de siguranță

În anumite cazuri atacurile cibernetice, cum sunt programele Ransomware, pot afecta chiar și un sistem actualizat. O a doua modalitate în care vă puteți proteja este făcând copii de siguranță a datelor. Acestea sunt copii ale informațiilor, stocate într-un loc diferit de calculatorul sau dispozitivul mobil personal. Atunci când pierdeți date prețioase, le puteți recupera din copiile de siguranță. Din păcate mult prea mulți oameni omit să facă regulat copii de siguranță, deși sunt simple și ieftine. Există două moduri de salvare a datelor proprii în copii de siguranță: pe suport de stocare fizic sau în mediul virtual de stocare bazat pe tehnologia Cloud. Fiecare dintre acestea are avantaje și dezavantaje. Puteți recurge la ambele variante în același timp, dacă nu sunteți siguri ce metodă să folosiți.

Soluțiile de stocare pe suport fizic sunt dispozitive pe care le aveți sub control, cum ar fi dispozitivele USB sau discurile conectate la rețea aflate la serviciu sau acasă. Avantajul folosirii de soluții fizice de stocare este acela că acestea vă permit să salvați și să recuperați volume mari de date foarte rapid. Dezavantajul aceste abordări este că, dacă sunteți afectați de programe malware cum sunt cele Ransomware, infecția se poate propaga și la copiile de siguranță. Dacă folosiți suport fizic pentru copiile de siguranță, trebuie să depozitați aceste copii într-un loc diferit, în siguranță. Asigurați-vă că orice copie este corect etichetată. Soluțiile bazate pe tehnologia Could sunt servicii online care permit stocarea și recuperarea copiilor de siguranță în rețeaua Internet. În mod uzual instalați un program pe calculatorul propriu iar acesta face totul. Avantajul soluției Cloud este simplitatea acesteia. În plus, dacă sunteți infectat cu programe Ransomware, acestea nu se pot propaga, în mod obișnuit, pe copiile de siguranță din mediul Cloud. Dezavantajul este că poate lua mult timp pentru realizarea copiilor de siguranță și recuperarea volumelor mari de date. Fiți siguri că ați studiat termenii de confidențialitate și securitate a datelor în cazul copiilor de siguranță aflată pe platforma Cloud. Oferă furnizorul soluției opțiuni de securizare puternice, cum ar fi criptarea datelor, sau mecanisme de autentificare puternice?

Atacurile de phishing

În fine, răufăcătorii își îmbunătățesc și schimbă metodele de atac în permanență. Infractorii folosesc deseori o altă metodă

Învățăminte de pe urma WannaCry

de atac, numită Phishing pentru a-și ataca și infecta victimele. Este un atac de Phising atunci când escrocii vă trimit un mesaj email ce încearcă să vă determine să deschideți un document atașat infectat sau să accesați un site compromis. Dacă faceți oricare dintre acestea, calculatorul personal va fi infectat. Deși „WannaCry" nu a folosit acest vector de atac, este folosit frecvent de multe alte tipuri de atacuri, inclusiv majoritatea programelor Ransomware. Mai mult, răufăcătorii care au creat „WannaCry" își vor modifica fără îndoială metodele de atac în lunile ce urmează și vor folosi noi tehnici, cum ar fi atacul de Phishing, pentru a infecta și mai multe calculatoare. Cheia pentru a vă proteja de astfel de atacuri bazate pe email este vigilența. Dacă un email sau un mesaj par ciudate, suspecte sau prea bune pentru ca să fie adevărate, atunci e vorba cel mai probabil de un atac.

Aflați mai multe

Abonați-vă la buletinul informativ lunar OUCH!, accesați arhiva și aflați mai multe despre programele de instruire asupra domeniului securității informației vizitând pagina web SANS securingthehuman.sans.org/ouch/archives

Versiunea în limba română

Cegeka este un furnizor independent de servicii IT&C ce își ajută clienții din întreaga Europă în transformarea lor digitală, dezvoltarea de aplicații folosind metodologiile Agile, soluții de încredere de tip Cloud și managementul serviciilor 24/7. Cegeka este prezentă în Austria, Belgia, Republica Cehă, Franța, Germania, Italia, Olanda, Polonia, România și Republica Slovacă, având 3600 de angajați. Cegeka a realizat o cifră de afaceri de 368 milioane de euro în 2015. Pentru mai multe informații vizitați www.cegeka.com.

Resurse

Ce sunt programele Malware:	https://securingthehuman.sans.org/ouch/2016#march2016
Despre Ransomware:	https://securingthehuman.sans.org/ouch/2016#august2016
Copiile de siguranță:	https://securingthehuman.sans.org/ouch/2015#august2015
Despre Phishing:	https://securingthehuman.sans.org/ouch/2015#december2015
Folosirea în siguranță a soluțiilor Cloud:	https://securingthehuman.sans.org/ouch/2016#november2016

Echipa editorială: Bill Wyman, Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley
Traducere: Cosmin Hănulescu