SANS SECURING THE HUMAN | ADVANCTION

OUCH! | Giugno 2017

La newsletter mensile sulla sicurezza informatica per tutti gli utenti

OUCH!

IN QUESTO NUMERO...

Una lezione da WannaCry

Introduzione

Di recente, avrete probabilmente sentito parlare dello straordinario attacco informatico chiamato “WannaCry” che si è reso responsabile del blocco di oltre 200.000 computer, cifrando i dati di moltissime aziende e organizzazioni, ivi inclusi alcuni ospedali del Regno Unito. Ci sono diversi motivi per cui questo attacco è assurto agli onori della cronaca: in primo luogo, si è diffuso rapidamente da computer a computer sfruttando una vulnerabilità presente nei computer Windows. In secondo luogo, l’attacco si è basato su un tipo di malware denominato “Ransomware”, in grado di infettare computer e crittografare tutti i file, impedendone l’utilizzo. L’unico modo per recuperare i dati è tramite un salvataggio effettuato in precedenza o il pagamento ai criminali di un riscatto di 300 dollari per decifrare i dati. Questo attacco non sarebbe mai dovuto accadere: la vulnerabilità che “WannaCry” ha sfruttato nei computer Windows era già nota e Microsoft aveva rilasciato una patch nei mesi precedenti. Molte organizzazioni purtroppo non si erano aggiornate o utilizzano ancora sistemi operativi obsoleti come Windows XP per i quali non esisteva un rimedio. Ecco tre semplici passi che potete seguire per assicurarvi che gli attacchi come “WannaCry” non vi colpiscano.

L’autore di questo numero

Il Dr. Johannes Ullrich è Direttore delle Ricerche del SANS Technology Institute e fondatore di DShield.org. nonchè responsabile del **SANS Internet Storm Center** che monitora le minacce alla cyber security. Tiene inoltre i corsi SANS di Web Application Security (**DEV522**), Intrusion Detection (**SEC503**) e IPv6 (**SEC546**).

Gli aggiornamenti

Innanzitutto, assicuratevi che computer, dispositivi mobili, applicazioni e qualsiasi altra cosa collegata a Internet sia aggiornata. I criminali informatici cercano costantemente nuove vulnerabilità nel software. Una volta individuate, utilizzano programmi speciali per attaccare i dispositivi degli utenti. Parallelemente, le aziende che hanno creato il software per i dispositivi che usiamo quotidianamente lavorano strenuamente per risolvere queste vulnerabilità attraverso il rilascio di aggiornamenti. Aggiornando costantemente computer e dispositivi mobili, sarà più difficile che qualcuno possa compromettere i vostri computer. Il dato allarmante sulla diffusione di WannaCry è che gli aggiornamenti per risolvere e arrestare questo attacco sono stati rilasciati quasi due mesi prima da Microsoft. Se aziende, privati e organizzazioni avessero aggiornato i propri computer, questo attacco non si sarebbe mai diffuso. Per garantire che i dispositivi rimangano aggiornati, è necessario abilitate l’aggiornamento automatico quando possibile. Questa regola si applica a quasi tutte le tecnologie connesse a una

Una lezione da WannaCry

rete, non solo i computer e i dispositivi mobili, ma anche i televisori collegati a Internet, i router domestici, le console di gioco o fra qualche tempo anche l'auto. Se i sistemi o i dispositivi sono così vecchi da non essere più supportati con aggiornamenti di sicurezza, come ad esempio Windows XP, sostituiteli con altri nuovi che siano supportati.

Il modo migliore per proteggersi da attacchi come Wannacry consiste nel mantenere i computer aggiornati, stare attenti agli attacchi phishing ed effettuare il savataggio di dati e sistemi.

I salvataggi

In alcuni casi, gli attacchi informatici come il Ransomware possono infettare anche sistemi aggiornati per cui è necessario adottare un metodo ulteriore per una protezione adeguata: il salvataggio dei dati (backup). I backup sono copie delle informazioni memorizzate in un luogo diverso dal computer o dal dispositivo mobile in modo che, semmai doveste perdere dei dati preziosi, sarà possibile recuperarli dai backup. Purtroppo, troppe persone non eseguono backup regolari, anche se si tratta di operazioni semplici e poco costose. Ci sono due modi per eseguire il backup dei dati: su supporti fisici o su cloud. Ogni approccio ha, naturalmente, vantaggi e svantaggi, ma potete utilizzarli entrambi contemporaneamente se non sapete quale scegliere.

Quando parliamo di supporti fisici intendiamo dispositivi come le unità USB esterne o le NAS, unità disco collegate alla rete, da casa o da ufficio. Il vantaggio di utilizzare i media fisici è che essi consentono di eseguire il backup e il recupero di grandi quantità di dati molto velocemente. Lo svantaggio di un tale approccio è che qualora veniste infettati da un malware, è possibile che l'infezione si diffonda sui vostri backup. Se utilizzate supporti fisici, è necessario memorizzare copie del backup in un altro luogo in una posizione protetta. Assicuratevi che i backup memorizzati siano correttamente etichettati. Le soluzioni basate su cloud, invece, sono servizi online che eseguono i salvataggi e memorizzano i file su Internet. In genere, si installa un programma sul computer che si occupa automaticamente della copia. Il vantaggio delle soluzioni cloud risiede nella loro semplicità. Inoltre, se si viene infettati da un Ransomware, l'infezione di solito non può accedere ai backup basati su Cloud. Tra gli svantaggi vi è però il lungo tempo richiesto sia per eseguire il backup sia per effettuare il ripristino di grosse quantità di dati. Assicuratevi di analizzare la privacy e la sicurezza dei servizi cloud, prima di attivarli, verificando, ad esempio, che il servizio di backup sia in grado di offrire una sicurezza forte, implementando la crittografia dei dati e l'autenticazione forte.

Una lezione da WannaCry

Il Phishing

I criminali informatici aggiornano e modificano continuamente i loro metodi di attacco. Un altro mezzo molto utilizzato per infettare le vittime è il Phishing che ha luogo quando un criminale vi invia un messaggio di posta elettronica con lo scopo di trarvi in inganno e farvi aprire un allegato infetto o visitare un sito dannoso. Sebbene WannaCry non abbia utilizzato questo metodo di attacco, si tratta comunque di un metodo comunemente usato anche per diffondere ransomware. È possibile che i criminali informatici che hanno sviluppato WannaCry aggiornino i loro metodi nei prossimi mesi utilizzando nuove tecniche come il phishing per riuscire a infettare sempre più computer. La chiave per proteggersi dagli attacchi che si diffondono via posta elettronica è il buon senso: se un messaggio sembra strano, sospetto o troppo bello per essere vero, si tratta probabilmente di un attacco.

Per saperne di più

Iscriviti ad OUCH!, la newsletter mensile dedicata alla security awareness, consulta i suoi archivi online, e scopri le soluzioni di SANS sulla security awareness visitando il sito
securingthehuman.sans.org/ouch/archives

Versione in Italiano

La versione in italiano è curata da Advanction S.A., un'azienda impegnata nella Sicurezza, nel Risk Management Operativo e nella Security Awareness. Seguila su www.advanction.com e su Twitter(@advanction).

Risorse

Il Malware:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201603_it.pdf
Il Ransomware:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201608_it.pdf
Salvataggi e ripristino:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201508_it.pdf
Il Phishing:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201512_it.pdf
Usare il cloud in modo sicuro:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201611_it.pdf

Direzione editoriale: Bill Wyman, Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley