M-SOFT, spol. s r.o.
ul. Jana Masaryka 12
586 01 Jihlava

IČO 49434853, tel. 567 579111, mail: maska@m-soft.cz

Vysočina, kraj
MUDr. Jiří Běhounek
Žižkova 57
587 33 Jihlava

Věc: Vyjádření k útoku hackerů z pátku 13. května 2016

Vážení,

na základě vašeho dotazu zasílám informace k útoku hackerů na některé prvky naší internetové sítě dne 13.5.2016.

Útok primárně postihnul přijímací/vysílací zařízení Nanostation a NanoBeam od výrobce Ubiquiti Networks Inc. Nejprve byla virem (označovaným Motherfucker) nakažena zařízení na veřejných IP adresách a z těchto zařízení byla následně nakažena i zařízení na neveřejných IP adresách ve vnitřní síti.

Útok nebyl veden proti naší síti ale proti zařízením výrobce Ubiquiti po celém světě, postiženi byly zejména ti operátoři, kteří provozovali alespoň část zařízení na veřejných IP adresách. Aktuální verze firmware zařízení Ubiquiti v den útoku (i většina předchozích verzí) obsahovala bezpečnostní chybu, která umožňovala se k zařízení připojit a nahrát do něj virus i bez znalosti přístupového hesla. Virus následně prozkoumával okolní síť a stejným způsobem se šířil na další nalezená zařízení. Později začal virus útočit i na DNS server sítě a další zařízení. Opravný firmware vydal výrobce zařízení do 2 dnů od počátku útoku, v té době již bylo velké množství zařízení nakaženo. Přesto se nám v následujících dnech podařilo z většiny zařízení virus vzdáleným přístupem vymazat a nahrát opravený firmware, který byl vůči případnému stejnému útoku odolný, navíc jsme změnili default porty, na kterých se k zařízením přistupovalo. U více než 2 tisíc jednotek jsme to však nestihli a zavirované jednotky provedly výmaz vlastní konfigurace a tím se odpojily od internetové sítě a již nebylo možno je vzdáleně opravit.

Zákazníky jsme o nastalé situaci informovali jednak pomocí SMS zprávy, webovou stránkou, mailem i pomocí sdělovacích prostředků takže každý zákazník se nějakou cestou dozvěděl, jak má v případě poruchy postupovat, neboť jsme nebyli schopni to v krátkém čase odbavit telefonicky jednoho po druhém.

Vytvořili jsme seznam linek s poruchou, většinu jich museli technici navštívit osobně. Přestože jsme na to nasadili všechny dostupné kapacity a sjednali jsme výpomoc i s některými dalšími firmami, trvalo odstranění poruch 12 dní. Nejprve jsme opravovali linky firemní a následně domácnosti, vždy naráz celé obce či části města abychom eliminovali čas na cestě, nejprve lokality s vysokou penetrací poruch a nakonec jednotlivce. Po zprovoznění všech linek jsme všechny zákazníky postižené výpadkem služby informovali o možnosti získat finanční kompenzaci za nefunkční

službu. Zatím si ji vyzvedla pouze menší část zákazníků ale konečný termín pro vyplacení kompenzací jsme stanovili na konec roku 2016.

Virus nenapadal data přenášená data takže privátní data zákazníků nebyla po celou dobu útoku či výpadku nikterak ohrožena, na což se mnozí z nich dotazovali v souvislosti např. s hesly k mailům, do internetového bankovnictví ap.

Analyzovali jsme záležitost z hlediska možné prevence problému i za předpokladu existence zásadní chyby ve firmware zařízení:

- při prvním útoku postačilo nepoužívat defaultní čísla portů pro management zařízení, my jsme bohužel používali defaultní, změnili jsme až při likvidaci útoku. Při druhém útoku, který následoval cca 3 týdny po prvním a který ve větší míře postihl jiného operátora z našeho regionu, jsme už odolali, protože jsme jednak používali nově vydaný fw bez předchozí díry a navíc jsme provedli další technická opatření, např. jsme omezili management pouze z vyjmenovaných IP.
- případné nepoužívání veřejných IP adres pro nás není vhodné, neboť zařízení Ubiquiti někdy slouží i jako NAT router a případné nahrazení tohoto zařízení jiným výrobcem by nezvýšilo úroveň bezpečnosti
- neumožnit vzájemnou komunikaci těchto zařízení, aby v případě napadení jednoho nebyl technicky možný přenos na zařízení sousední a následek případného útoku byl malý a rychle řešitelný
- sledování anomálií v provozu sítě, někdy se tak podaří včas podchytit vznikající problém, my monitorujeme systémem FlowMon.
- použití systému automatické detekce a blokace alespoň některých útoků, zejména DoS a DDoS, u nás používáme zařízení DefensePro od firmy Radware. V případě výše popisovaného útoku nebylo schopno zabránit nakažení jednotek virem, neboť to ještě nebyl DoS útok, ale následný DDoS útok na náš DNS server už zachytilo a upozornilo nás na problém.

Obecně platí, že při návrhu a provozu velké sítě je potřeba promýšlet nejen základní funkčnost a kapacitu (aby vše komunikovalo) ale stále přemýšlet i co by mi jako hackerovi ztížilo práci či mne odradilo od útoku. Na počátku to sice přinese vyšší náklady a více práce ale z dlouhodobého hlediska je to nejenom bezpečnější ale i ekonomičtější oproti nákladům na odstraňování následků.

S pozdravem

V Jihlavě dne 18.7.2016

Ing. Bohuslav Maška
jednatel