Celý rozsah IP adres Wedosu se dostal na blacklist, zákazníkům se ztrácela pošta

lupa.cz/clanky/cely-rozsah-ip-adres-wedosu-se-dostal-na-blacklist-zakaznikum-se-ztracela-posta

Martin Drtina

Lupa.cz »

Autor: Wedos
Datacentrum Wedos

Podle vysvětlení hostingu šlo o penalizaci za tři izolované kyberincidenty. Zkušenosti oslovených expertů ukazují, že může jít o vážnější problém.

Úspěšný útok na trojici VPS serverů provozovaných hostingem Wedos vedl k zařazení celého firmou používaného rozsahu IP adres na blacklist. V důsledku toho se ostatní zákazníci tohoto providera, kteří s původním incidentem a napadenými stroji neměli nic společného, dostali na měsíc do situace, že jejich e-maily byly ve vší tichosti zahazovány jako nedoručitelné. Jiné pak končily kvůli penalizacím za blacklist ve složce se spamem.

S touto nedávnou zkušeností se redakci přihlásil zákazník Wedosu, který si nepřál být jmenován. Jeho totožnost známe, požadavek však respektujeme. Říkejme mu proto třeba pan Radek.

Nic jste neprovedl, přesto vás blokují

„Poslední víc než měsíc e-maily ode mě padaly některým lidem do spamu, nebo dokonce nebyly doručené vůbec. Když už mi došla trpělivost, začal jsem to řešit s podporou," popisuje pan Radek své peripetie s VPS serverem, který u Wedosu hostoval. Problémy s doručitelností zaznamenával hlavně u elektronické pošty doručované do domén přiřazených ke cloudu Office 365. Naproti tomu do Gmailu nebo e-mailů provozovaných na samostatných mailserverech zprávy dál docházely.

Radek si na radu technické podpory zkusil ze svého stroje poslat e-mail na cloud u Microsoftu. Z hlavičky zprávy, která skončila ve spamu, pak technik zjistil zařazení IP adresy na spamlist Uceprotect.net. „Bohužel kvůli jejich politice klasifikace spamů jsme se dostali bez varování ihned na L3 listing, u kterého je nutné vyčkat určitý časový úsek, než proběhne delistování," odpověděla technická podpora providera. „Na to konto jsem řekl, že chci ukončit službu a vrátit peníze. Odpověděli, že službu můžu nechat rok doběhnout," doplnil Radek.

Wedos problém potvrzuje. „V nedávné době byla naše společnost zařazena na blacklist uceprotect.net na L3 úrovni," reagoval na dotazy Lupy za providera Ivan Sárközi s tím, že blacklistován byl celý adresní rozsah Wedosu. „Uceprotect.net absolutně nerespektuje, že v našich IP rozsazích se nachází několik stovek tisíc MX záznamů pro různé domény, které bezproblémově zajišťují e-mailový provoz," dodal Sárközi. Podnětem k penalizaci celého autonomního rozsahu Wedosu měly být kybernetické incidenty na stroje jiných klientů. „Došlo k napadení tří VPS našich zákazníků, na což jsme bezprostředně zareagovali a dotčené servery byly okamžitě odpojeny od sítě," ubezpečil.

Přesunout mailserver jinam nestačí

Ztrácející se poštu chtěl pan Radek řešit migrací mailhostingu do cloudu Googlu a posléze i na Office 365. Ani jedno z toho ale nepomohlo. Test doručitelnosti přes službu MailGenius ukázal, že změnit pouze MX řádky v DNS záznamech nestačí. „Jako problém se ukázalo, že moje doména má A záznam nasměrovaný na IP adresu z rozsahu, který spravuje Wedos," neskrýval Radek překvapení nad přísností klasifikačních pravidel.

Zkusil proto vzniklou situaci s blacklistem Uceprotect.net vyřešit sám, ale s pokusy o odstranění IP adresy z blokace narazil. „Z blacklistu může odebrat IP adresy jen ten, kdo je spravuje. Ne samotný zákazník," zjistil Radek. Wedos podle něj mohl odblokování adres

uspíšit zaplacením 85 švýcarských franků. „To ale evidentně neudělali a čekali týden, jestli IP adresy ze seznamu nezmizí," dodal s tím, že jako zákazník doplácí na to, že si společnost neohlídala kybernetickou bezpečnost a dostala tím do problémů všechny ostatní klienty.

Zařazení celého adresního rozsahu na blacklist považuje Wedos za nepřiměřený krok a finanční poplatek za „vysoce neetickou praktiku". A chce se bránit. „Zvažujeme další právní možnosti proti tomuto typu chování, které bychom označili za nekalé. Nejedná se přitom o první pochybné zařazení z jejich strany," upozornil Sárközi.

Pochopení pro toto vysvětlení a postup hostingu Radek nenašel. „Ušetřili sice pár desítek franků, ale zaplatilo za to těch několik stovek tisíc MX záznamů pro různé domény," uzavírá s tím, že nakonec zmigroval všechny u Wedosu hostované služby jinam.

Ostatní sází na proaktivní přístup a monitoring

Nakolik je reálná hrozba, že vinou několika špatně zabezpečených serverů se do digitální klatby pro elektronickou poštu dostanou i stroje všech ostatních zákazníků stejného providera, a zdali tomu lze aktivně předcházet, jsme zjišťovali u provozovatelů dvou velkých datacenter v Praze – MasterDC a Greenhousing (DC6).

„Uceprotect je jeden ze známějších a u nás populárních systémů. K blacklistování celého rozsahu nedochází okamžitě po prvním či ojedinělém porušení. Podle našich zkušeností pracuje s eskalací ve třech úrovních – napřed blokuje konkrétní IP adresu, pak určitý rozsah a až v poslední instanci podniká opatření vůči všem adresám daného autonomního systému," vysvětluje za MasterDC Michaela Rabasová.

Toto datové centrum proaktivně zalistování IP adres na různé blacklisty sleduje. „Disponujeme monitoring účtem a o umístění IP adres z našeho rozsahu víme ještě dříve, než k němu reálně dojde," vysvětluje Rabasová. Zjištěná pochybení jsou pak se zákazníky

řešena individuálně. Dalším preventivním opatřením je, že novým zákazníkům je u automatizovaně zřizovaných VPS serverů rozesílání pošty právě z těchto důvodů zakázáno.

Také jednatel Greenhousingu Zdeněk Maršál nevěří tomu, že by Wedos byl blokací celého autonomního systému potrestán při prvním pochybení. „Obvykle se jedná o vícestupňový, částečně automatizovaný proces. Při každém zjištěném prohřešku bývá administrativní kontakt příslušné IP adresy nebo rozsahu upozorněn a má možnost reagovat," objasňuje zažitou praxi. Vzhledem k tomu, že existují přibližně dvě stovky různých blokačních seznamů, které mají různý účel a význam, liší se jak kritéria pro zařazení na takový seznam, tak podmínky pro následný delisting.

„Je rovněž zřejmé, že zařazení na více blocklistů současně, a to ne jednou IP adresou, ale celým rozsahem, obvykle signalizuje zásadní selhání ve standardních provozních postupech a dlouhodobou ignoraci varování. Řešení takové situace je mnohem obtížnější než včasná detekce a náprava potenciálních incidentů," vypočítává Maršál.

DC6 podobně jako konkurenční MasterDC také automaticky monitoruje všechny relevantní blacklisty a okamžitě informuje zákazníky o zjištěných incidentech. „Naše obchodní podmínky nám umožňují v krajním případě omezit provoz zákazníka, který buď porušuje pravidla, nebo svou laxností umožňuje jejich porušení třetí stranou," naráží šéf Greenhousingu na to, že ve většině případů není zákazník útočníkem, ale obětí zneužívání jeho zdrojů kvůli narušení bezpečnosti jeho systémů. „Jednoduše je hacknut a jeho zařízení je používáno bez jeho vědomí," dovysvětlil.

Blacklist Uceprotect eviduje v seznamu 62 tisíc samostatných IP adres a přes tisícovku autonomních systémů.

- Chcete mít **Lupu bez bannerů?**

- Chcete dostávat speciální týdenní **newsletter o zákulisí českého internetu?**
- Chcete mít k dispozici **strojové přepisy podcastů?**
- Chcete dostávat **exkluzivní tištěný speciál Lupa 3.0?**
- Chcete získat slevu **1 000 Kč na jednu z našich konferencí?**

Staňte se naším podporovatelem

Chci se stát podporovatelem

Regulace fakt není pro firmy pohoda jazz

Vstoupit do diskuse (37 názorů)

Byl pro vás článek přínosný?

+40

To fakt nevim, kam vlastne lezete. uceprotect https ma... mozna tam neni redirect, ale to muj prohlizec se s tim popere a https sam vynucuje.

Danny