Ochrana před DDOS útoky

Lépe čelit DoS a DDoS útokům mířícím na internetové služby populární v České republice. To je hlavním úkolem projektu Bezpečná VLAN, který nedávno spustilo šest velkých hráčů českého internetu.

Projekt vznikl na půdě sdružení NIX.CZ a je reakcí především na intenzivní DoS útoky z března minulého roku. Mezi šestici zakládajících členů patří i webhostingová společnost Active 24. Význam Bezpečné VLAN přiblížil v rozhovoru její technický ředitel Zdeněk Brůna.

» Proč projekt vznik a čeho má dosáhnout?
Impulzem pro spuštění projektu byly intenzivní DoS útoky z března 2013. Aktivní členové NIX.CZ nechtěli jen sedět s rukama založenýma v klíně a čekat na další a možná i rozsáhlejší útoky, chtěli zlepšit svoji schopnost čelit jim. Proto když přišel člen představenstva NIX.CZ Ondřej Filip s konkrétními nápady, jaká opatření nasadit, měl ihned velkou podporu a prvotní nápad se velmi rychle rozvinul do současné podoby. Bezpečná VLAN má sloužit jako nouzový prostředek vzájemné komunikace členů a zákazníků sdružení NIX.CZ s vysokým prvkem důvěry a zabezpečení pro případ masivních útoků na internetovou infrastrukturu. Smyslem vzniku Bezpečné VLAN bylo umožnit spojení poslední šance („last resort") v případě, že se infrastruktura člena Bezpečné VLAN stane cílem útoku. Jednoduše řečeno, má členům Bezpečné VLAN zajistit aspoň nějakou konektivitu, když ostatní nebudou mít žádnou. Členství je podmíněné zavedením a dodržováním celé řady bezpečnostních opatření, a s přibývajícími členy tedy poroste internetová bezpečnost obecně.

» Které společnosti se podílejí na projektu Bezpečná VLAN a co mu přinášejí?
Zakládajících členů je šest. Jsou jimi Active 24, Cesnet, CZ.NIC, Dial Telecom, Seznam.cz a Telefónica ČR. Šest není mnoho, i když se jedná o velmi významné subjekty působící na českém internetu. Zastupují ale jak svět poskytovatelů připojení (Dial Telecom a Telefónica), poskytovatele obsahu (Active 24 a Seznam.cz), akademickou sféru (Cesnet) a v neposlední řadě i provozovatele centrálního registru domén .cz (CZ.NIC).

Hlavním přínosem těchto subjektů je, že projekt aktivně nejen podporují, ale pomohli jej nastartovat. Zejména aktivní účastí na pracovních skupinách NIX.CZ, spoluprací na definici pravidel pro vstup do Bezpečné VLAN nebo jejich samotným zavedením a dodržováním uvnitř svých organizací.

Zakládající členové dále silou svých značek zvyšují význam Bezpečné VLAN, a tedy i zájem ostatních do ní vstoupit, což je samozřejmě další významný přínos zmíněných společností. A to i přes to, nebo možná právě proto, že vstup není v žádném případě formální záležitostí.

» Na jakém principu projekt funguje?
Pro vysvětlení opusťme na chvíli svět technologií a internetu. Představme si situaci, kdy se zraníte na malíčku u nohy a do rány se dostane smrtelná infekce, která se dokáže velmi rychle šířit po celém těle. Jedinou možnou záchranou života bude amputace části končetiny. Budete s akceptací tohoto řešení váhat? Bezpečná VLAN se připravuje přesně na takto vážnou situaci, ale v oblasti internetu. Buď necháme DoS volně šířit internetem a postupně jej celý položit, nebo se oddělí „zdravá" část sítě od té „nemocné" a bude zachován provoz internetu aspoň v omezeném režimu. V extrémním případě tak bude fungovat spojení jen mezi členy Bezpečné VLAN, ale při rozsáhlém útoku budeme rádi aspoň za to. Na rozdíl od amputované končetiny můžete odříznuté sítě po vyřešení problémů jednoduše zase připojit, takže se nejedná zase o tak dramatický příběh. Navíc je důležité zmínit, že každý člen má ve své moci rozhodnutí, zda a kdy se odpojí

Na rozdíl od amputované končetiny můžete odříznuté sítě po vyřešení problémů jednoduše zase připojit

AUTOR
Jan Spěšný
editor Connectu

Active 24

Společnost **Active 24** patří mezi největší české poskytovatele webhostingových služeb, serverových řešení a registrátory domén. Služby **Active 24** se vyznačují vysokou profesionalitou a technickou kvalitou. Firma působí na trhu už sedmnáct let a kromě poskytování služeb více než 70 tisícům zákazníků se vždy firma snažila pozitivně přispívat k rozvoji českého IT a internetového prostředí. Mezi nejvýznamnější aktivity z této oblasti posledních let patří například projekty DNSSEC, IPv6, CSIRT nebo bezpečná VLAN.

od zbytku internetu a zůstane připojen pouze v Bezpečné VLAN. Bezpečnou VLAN si řídí sami její členové, jsou nezávislí na NIX.CZ.

» Co konkrétně pro vás účast na projektu znamená a co jste museli pro vstup do něj udělat?
Předně to vnímáme jako velmi prestižní záležitost. Jako ocenění toho, jak ke zvyšování internetové bezpečnosti dlouhodobě přispíváme.

Se zaváděním opatření potřebných pro vstup do projektu jsme začali už v době, kdy se o ní ani zdaleka nemluvilo. V našem případě mohu uvést tři konkrétní příklady. Prvním je zavedení aktivní podpory DNSSEC pro domény .cz v roce 2008, kterou jsme ohlásili jako první z českých registrátorů. Druhou akcí, která nám pomohla zlepšit naši schopnost efektivně komunikovat v případě bezpečnostního incidentu, bylo vytvoření našeho CSIRT týmu v roce 2012. A opět jsme byli první mezi komerčními firmami u nás, kdo měl ustanoven oficiální CSIRT tým. Třetím příkladem budiž naše již dlouholeté využívání standardu BCP38. Díky tomu filtrujeme odchozí provoz ze své sítě tak, aby zabránil odesílání paketů s podvrženou hlavičkou odesílatele (IP spoofing), a tím i šíření DoS. Některým dalším podmínkám, které bylo nutno splnit pro vstup do tohoto VIP klubu, jsme jednoduše vyhověli proto, že jsme dlouhodobě považováni za důvěryhodného partnera, který aktivně pomáhá rozvoji sdružení NIX.CZ, a tedy i českého internetu.

Samozřejmě jsme ještě před nedávnem nesplňovali všechny podmínky nutné pro vstup do Bezpečné VLAN, je jich skutečně celá řada. Na konci roku 2013 jsme tak například zaváděli Response rate limiting a na IPv6 pak Control plane policy. Tedy opatření, která, velmi zjednodušeně řečeno, účinně snižují možnosti šíření útoků typu DDoS/DoS.

» Co díky členství můžete nabídnout svým klientům?
Větší bezpečnost, spolehlivost a dostupnost pro jejich webové prezentace, e-mailové služby, e-shopy a další služby, které jsou hostovány u nás. Mám na mysli zejména lepší ochranu před útoky typu DDoS/DoS, které by znamenaly nedostupnost námi poskytovaných služeb. V současné době jsme jedinou webhostingovou společností, která je v Bezpečné VLAN zapojena.

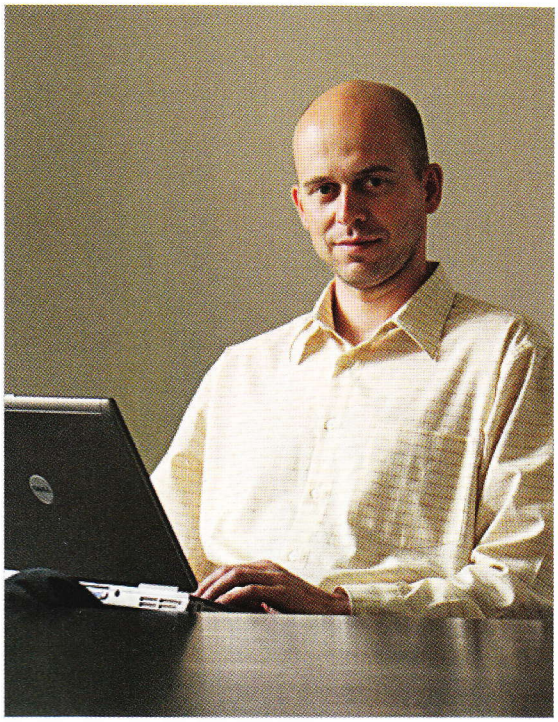
» Dotkne se spolupráce společností zapojených do projektu nějak i bezpečnosti českých webů, které nejsou provozovány členem Bezpečné VLAN?
I když je Bezpečná VLAN vybudována uvnitř NIX.CZ, jednou ze základních podmínek bylo, aby její existence nijak neovlivňovala stávající běžný provoz členů NIX.CZ, kteří nebudou na projektu participovat. Ke zvýšení bezpečnosti ale dojde v podstatě pro všechny, protože velká část zaváděných opatření zabraňuje šíření DoS útoků mezi jednotlivými peeringovými partnery. Sníží se tak riziko příchodu DoS útoku ze sítí členů, což bude prospěšné pro všechny. Samozřejmě platí, že k výraznému zlepšení dojde až při velkém počtu zapojených subjektů v tomto projektu.

Ale už samotné definování pravidel nutných pro vstup pomohlo zvýšit bezpečnost všech. Operátoři mají totiž lepší možnost zjistit, jaká opatření je vhodné zavést. Každý, kdo pak na základě tohoto podnětu reálně zavede aspoň některá z nich, například zmiňované BCP38, pomáhá zvýšení bezpečnosti na internetu, a to i bez nutnosti zapojení se do Bezpečné VLAN.

» Jakým způsobem a za jakých podmínek se k projektu mohou připojit další společnosti?
Podmínky přijetí nového člena jsou stejně jako pravidla pro připojení do Bezpečné VLAN pro všechny identické a veřejně dostupné na adrese www.nix.cz. Žadatel musí být připojen do NIX.CZ aspoň půl roku a musí se písemně zavázat, že v případě přijetí bude dodržovat všechna pravidla pro připojení do Bezpečné VLAN. Důležitými podmínkami je také předložení doporučení na přijetí od nejméně dvou stávajících členů a neobdržení veta přijetí od nejméně jedné šestiny stávajících členů. Důvěra mezi členy musí být na nejvyšší možné úrovni, proto tento systém doporučení vítáme. Žadatel dále musí splnit všechny uvedené technické a organizační podmínky, k čemuž se zavázal, protože se bude jejich dodržování kontrolovat. Vstup je tedy opravdu poměrně komplikovaný, ale o to větším lákadlem tak pro potenciální zájemce je.

» Co jim členství přináší?
Svým členům přináší především marketingovou výhodu, možnost kvalitativně se odlišit se od konkurentů. Na našem přeplněném trhu internetových poskytovatelů se podobných příležitostí nenachází mnoho. Být v exkluzivní společnosti bezpečných poskytovatelů má svoji váhu.

» Existují už nějaké konkrétní výsledky spolupráce na projektu?
Myslím, že největším přínosem je sám fakt, že se o zvýšení bezpečnosti nyní daleko více hovoří. A nejen to. Zájem o vstup do Bezpečné VLAN spustil u mnoha internetových poskytovatelů zavádění bezpečnostních opatření, a bezpečnost českého internetu se tedy již nyní začala zlepšovat. Dalším přínosem, který osobně velmi vítám, je to, že se daleko lépe dokážeme domluvit se subjekty, jež jsou do projektu zapojeny. Lépe se známe a máme společný cíl. Našim síťovým specialistům to zase přineslo zajímavé rozšíření jejich obzorů, zkušeností a znalostí.


Technický ředitel Active 24 Zdeněk Brůna

Zájem o vstup do Bezpečné VLAN spustil u mnoha internetových poskytovatelů zavádění bezpečnostních opatření, a bezpečnost českého internetu se tedy již nyní začala zlepšovat

Další přínosy přijdou brzy. Konkrétní spolupráce, fungování v rámci Bezpečné VLAN, ale také kontrola dodržování pravidel se upřesňují už nyní.

» Máte informace o dalších subjektech, které by do projektu chtěly vstoupit?
Jsem mile překvapen, jak velký zájem Bezpečná VLAN vyvolala. Nechtěl bych ale jmenovat konkrétní subjekty. Mluví se však nejméně o dalších deseti vážných zájemcích, kteří se na vstup nyní připravují. Držíme jim palce a pomáháme jim. Nedávno jsme zabezpečili jednomu takovému zájemci jeho primární doménu pomocí DNSSEC, což je jednou z podmínek vstupu do Bezpečné VLAN. Na můj dotaz, proč tak činí zrovna nyní a proč s tím tak spěchá, jsem obdržel jasnou odpověď: „Chceme se dostat k vám do klubu." ■