Pravidla pro připojení do Bezpečné VLAN

ACTIVE 24, s.r.o., se sídlem Sokolovská 394/17, Praha 8, IČ 25115804,
CESNET, z.s.p.o., se sídlem Zikova 4, Praha 6, IČ 63839172,
CZ.NIC, z.s.p.o., se sídlem Americká 23, Praha 2, IČ 67985726,
Dial Telecom, a.s., se sídlem Křižíkova 237/36a, Praha 8, IČ 28175492,
Seznam.cz, a.s., se sídlem Radlická 3294/10, Praha 5, IČ 26168685 a
Telefónica Czech Republic, a.s., se sídlem Za Brumlovkou 266/2, Praha 4, IČ 60193336

(společně dále jen „**Zakladatelé**“)

za účasti **NIX.CZ, z.s.p.o.**, se sídlem Vinohradská 184, Praha 3, IČ 65990471,

tímto schvalují tato Pravidla pro připojení do Bezpečné VLAN na platformě NIX.CZ z.s.p.o. (dále jen „**Pravidla**“).

1. ÚVODNÍ USTANOVENÍ

1.1. Tato Pravidla upravují podmínky připojení do Bezpečné VLAN zřízené shora uvedenými zakladateli v rámci NIX.CZ, z.s.p.o. (dále jen „**BV**“).

1.2. BV se zřizuje v souladu s Platným provozním řádem a ceníkem služeb a stanovami NIX.CZ, z.s.p.o. (dále jen „**NIX.CZ**“).

1.3. Tato Pravidla se v plném rozsahu vztahují i na Zakladatele, a to včetně případného vyloučení z BV.

1.4. BV slouží jako nouzový prostředek vzájemné komunikace členů a zákazníků sdružení NIX.CZ s vysokým prvkem důvěry a zabezpečení pro případ masivních útoků na internetovou infrastrukturu.

1.5. Smyslem vzniku BV je umožnit spojení poslední šance („last resort“) v případě, že se infrastruktura člena BV stane cílem útoku.

1.6. Připojení do BV je bezplatné.

1.7. NIX.CZ není Zakladatelem, je však součástí BV, může do ní být kdykoliv připojen a je oprávněn ji užívat stejně jako členové BV.

2. PODMÍNKY ZAŘAZENÍ NOVÝCH ČLENŮ ČI ZÁKAZNÍKŮ NIX.CZ DO BV

2.1. Členem BV se může stát jen člen nebo zákazník, který je připojen do jakéhokoliv uzlu NIX.CZ déle než 6 měsíců.

2.2. Žadatel o členství v BV se musí písemně zavázat, že v případě přijetí do BV bude dodržovat Pravidla. Musí rovněž předložit doporučení nejméně dvou stávajících členů BV k přijetí do BV, čestné prohlášení k doložení splnění podmínek dle článku 3 a kopii svých vzorových smluv či smluvních podmínek se zákazníky.

2.3. K žádosti o členství v BV se může vyjádřit kterýkoliv stávající člen BV. V případě, že ve lhůtě 7 dnů ode dne informování stávajících členů BV o žádosti o členství nebude nejméně jednou šestinou stávajících členů vznesen protest, může být žadatel do BV připojen a stát se jejím členem. Na přijetí do BV není dán právní nárok ani v případě, že jsou splněny všechny podmínky dle článku 2.5.

2.4. Členem BV se nemůže stát zákazník NIX.CZ, který je v rámci partnerského programu připojen do uzlu NIX.CZ prostřednictvím jiného člena či zákazníka NIX.CZ jako partnera.

2.5. Platnou žádost o připojení do BV může podat člen nebo zákazník NIX.CZ, který

2.5.1. se aktivně účastní pracovních skupin a hlasování v orgánech NIX.CZ, a to alespoň jednou ročně;

2.5.2. nemá vůči NIX.CZ žádné závazky po lhůtě splatnosti a v posledních 6 měsících neměl vůči NIX.CZ žádné závazky po lhůtě splatnosti po dobu delší než 14 dnů;

2.5.3. se nedopouští, a v minulosti se nedopustil, opakovaného ani podstatného porušení provozního řádu NIX.CZ či stanov NIX.CZ;

2.5.4. provozuje plně redundantní, nepřetížené, přípojky do nejméně dvou uzlů NIX.CZ tak, aby v případě výpadku všech přípojek do jednoho uzlu NIX.CZ byly ostatní schopny převzít a přenést bez přetížení veškerý běžný datový provoz;

2.5.5. smluvně zakazuje svým zákazníkům zneužívání sítě (spamming, útoky apod.);

2.5.6. provozuje ve své síti zároveň protokol IPv4 i IPv6, přičemž oba protokoly aktivně užívá k propojení do uzlů NIX.CZ, jejich prostřednictvím zpřístupňuje své webové prezentace, a přiděluje je svým zákazníkům;

2.5.7. má své domény, pod kterými komunikuje se svými zákazníky či obchodními partnery (včetně webů společnosti a produktových webů), podepsané pomocí technologie DNSSEC, s výjimkou situací, kdy nasazení podepisování brání vážné technické důvody, a má zapnutou validaci na resolverech;

2.5.8. má dohledové středisko (NOC) bezproblémově fungující v režimu 24x7 s e-mailovým kontaktem a nejméně dvěma platnými telefonickými kontakty (alespoň s jedním technicky nezávislým na protokolu IP) zveřejněnými v intranetu NIX.CZ, přičemž telefonické spojení je směřováno přímo na techniky schopné řešit problém a nesmí být realizováno přes IVR;

2.5.9. ve své síti používá filtrování zdrojových adres (zabránění IP spoofingu) ve smyslu BCP-38 či SAC004. Pro IP adresy v rámci vlastních AS musí být granularita alespoň /24 u IPv4 a /48 u IPv6;

2.5.10. má systém na detekci a likvidaci zdrojů útoku typu DNS amplification (zákaz nespravovaných otevřených resolverů, implementace response rate limiting);

2.5.11. monitoruje páteřní linky i zákaznické přípojky alespoň z hlediska toků a přenášených packetů (například MRTG či obdobné), monitoring musí umět aktivně upozornit na vybočení sledovaných hodnot z běžného intervalu;

2.5.12. nepropaguje pomocí BGP protokolu jiné rozsahy, než ke kterým je oprávněn;

2.5.13. neposílá ze své sítě provoz z rozsahů, které nepropaguje;

2.5.14. své routery chrání v souladu s doporučením RFC6192 (control plane policy);

2.5.15. provozuje CERT/CSIRT tým, alespoň se statusem „listed“ u úřadu Trusted Introducer (http://www.trusted-introducer.org);

2.5.16. má zavedeny vnitřní procesy pro řešení incidentů;

2.5.17. zahájí práce na odstranění/omezení bezpečnostního incidentu co nejrychleji, nejpozději do 30 minut od jeho nahlášení;

2.5.18. sleduje bezpečnostní oznámení dodavatelů svých síťových komponent a patřičně na ně reaguje.

3. PROVOZNÍ PODMÍNKY PŘIPOJENÍ DO BV

3.1. Člen BV

3.1.1. se aktivně účastní pracovních skupin a hlasování v rámci BV;

3.1.2. monitoruje komunikaci speciálních e-mailových konferencí (mailing list) určených pro členy BV;

3.1.3. je zapojen do systému RTBH filteringu (Remotely-Triggered Black Hole Filtering), kterým se rozumí technika pro zmírnění dopadu DDoS útoků, jejímž prostřednictvím může síť, která je cílem útoku, za pomocí označení určenou BGP komunitou určit, která část provozu se bude blokovat na straně NIX.CZ;

3.1.4. využívá Route Serveru provozovaného v rámci BV, a to zejména k zapojení do systému RTBH filteringu popsaných v článku 3.1.3 a k propojení s ostatními členy BV.

3.2. Připojení prostřednictvím BV by nemělo být užíváno jako hlavní propojovací platforma pro připojení do uzlu NIX.CZ, pokud k tomu není technický důvod, který člen BV oznámí do mailing listu.

3.3. Zapojení do BV je realizováno prostřednictvím fyzického portu nebo prostřednictvím 802.1Q.

3.4. BGP relace v rámci BV jsou chráněny proti session hijackingu například pomocí TCP MD5 signatur (RFC2385).

3.5. Člen BV smí do BV propagovat pouze prefixy, u kterých je schopen zaručit přiměřené aplikování pravidel dle článku 2.5 a článku 3.

4. DOHLED NAD DODRŽOVÁNÍM PRAVIDEL

4.1. Na dodržování Pravidel dohlíží zaměstnanci NIX.CZ, kteří jsou oprávněni průběžně testovat plnění těchto Pravidel (NIX.CZ je oprávněn při takovém testování Pravidla porušit). Zjištěná porušení budou oznamovat členům BV. Dotčený člen je oprávněn se k učiněným zjištěním vyjádřit; ostatní členové mohou požadovat vysvětlení či doplnění takových zjištění.

4.2. V případě porušení Pravidel, včetně případů, kdy člen BV přestane splňovat podmínky v článku 3, může ředitel NIX.CZ rozhodnout o vyloučení člena z BV. Opětovný vstup do BV je pak možný jen postupem dle článku 2.

5. ZMĚNY PRAVIDEL A JINÁ ROZHODOVÁNÍ; KOMUNIKACE

5.1. Změnu Pravidel může navrhnout kterýkoliv člen BV. Po prodiskutování návrhu vyzve ředitel NIX.CZ členy BV k hlasování. Návrh změny je přijat, pokud se pro něj vysloví nadpoloviční většina všech členů BV.

5.2. Veškerá komunikace členů BV probíhá prostřednictvím zvláštní e-mailové konference členů BV.

5.3. Každý člen BV je povinen poskytovat ostatním členům informace o významných bezpečnostních incidentech, k jejichž předcházení či řešení je BV určena.

5.4. Hlasování členů BV probíhá prostřednictvím elektronického hlasovacího systému zavedeného NIX.CZ.

5.5. Člen BV je povinen zachovávat mlčenlivost o skutečnostech, o kterých se dozvěděl v rámci svého členství v BV, zejména o veškerých informacích vyměňovaných mezi členy v rámci vzájemné komunikace, o zjištěných bezpečnostních incidentech v sítích jiných členů, o plnění nebo neplnění podmínek dle těchto Pravidel, jakož i o odmítnutí žadatele o členství v BV. Tyto informace lze uveřejnit pouze pokud dotčený člen udělil výslovný souhlas se zveřejněním a v případě, že původce informace není znám, souhlas se zveřejněním dali všichni členové BV.

5.6. V případě sporu o výkladu některého z ustanovení těchto Pravidel, zejména v případě posouzení, zda došlo k porušení některého z ustanovení těchto Pravidel, rozhoduje ředitel NIX.CZ.

6. PUBLICITA

6.1. Každý člen BV má právo užívat zvláštní logo BV v provedení schváleném členy BV.

6.2. Členové BV jsou uvedeni ve zvláštním seznamu členů BV umístěném na webu NIX.CZ a vysvětlujícím význam BV.

ACTIVE 24, s.r.o.

V Praze dne __.__._____

_____

Ing. Petr Šmída
jednatel

CESNET z.s.p.o.

V Praze dne __.__._____

_____

Ing. Jan Gruntorád, CSc.
ředitel sdružení

CZ.NIC, z.s.p.o.

V Praze dne __.__._____

_____

Mgr. Ondřej Filip, MBA
ředitel sdružení

Dial Telecom a.s.

V Praze dne __.__._____

_____

Zbyněk Pospíchal
na základě plné moci

Seznam.cz, a.s.

V Praze dne __.__._____

_____

Vlastimil Pečínka
technický ředitel

Telefónica Czech Republic, a.s.

V Praze dne __.__._____

_____

Ing. Petr Slováček
2. místopředseda představenstva

NIX.CZ, z.s.p.o.

V Praze dne __.__._____

_____

Martin Semrád
ředitel sdružení