**Čestné prohlášení žadatele o členství v projektu FENIX (Bezpečné VLAN)**

Společnost: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

IČ: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Sídlo: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Zastoupený \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(dále jen „Žadatel“)

Žadatel žádá o členství v projektu FENIX (Bezpečné VLAN) zřízeného v rámci NIX.CZ, z.s.p.o. (dále jen „BV“) v souladu s Pravidly pro připojení do FENIX (Bezpečné VLAN) (dále jen „Pravidla“).

Žadatel prohlašuje, že

1. se nedopouští, a v minulosti se nedopustil, opakovaného ani podstatného porušení provozního řádu NIX.CZ či stanov NIX.CZ;
2. provozuje plně redundantní, nepřetížené, a na sobě nezávislé přípojky do nejméně dvou uzlů NIX.CZ tak, aby v případě výpadku všech přípojek do jednoho uzlu NIX.CZ byly ostatní schopny automaticky převzít a přenést bez přetížení veškerý datový provoz vyměňovaný s partnery v NIX.CZ;
3. smluvně zakazuje svým zákazníkům zneužívání sítě (spamming, útoky apod.);
4. 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;

|  |  |
| --- | --- |
| Seznam webových prezentací: |  |

1. provozuje CERT/CSIRT tým, alespoň se statusem „listed“ u úřadu Trusted Introducer;

|  |  |
| --- | --- |
| Oficiální název týmu: |  |

1. 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;

|  |  |  |
| --- | --- | --- |
| Seznam domén podepsaných DNSSEC | Seznam domén nepodepsaných DNSSEC | Důvody nepodepsání |
|  |  |  |

1. má dohledové středisko (NOC) bezproblémově fungující v režimu 24x7 s alespoň jedním telefonickým kontaktem bez obtíží dosažitelným i v případě masivního DDoS útoku na internetovou infrastrukturu člena zveřejněným v intranetu NIX.CZ, přičemž telefonické spojení je směřováno přímo na techniky schopné řešit problém a nesmí být realizováno přes IVR;
2. ve své síti používá filtrování zdrojových adres (zabránění IP spoofingu) ve smyslu BCP-38 či SAC004. Pro IP adresy v rámci vlastních AS je granularita alespoň /24 u IPv4 a /48 u IPv6;
3. má systém na detekci a likvidaci zdrojů útoku typ amplification (například DNS, SNMP, NTP, zákaz nespravovaných otevřených resolverů, implementace response rate limiting);
4. monitoruje páteřní linky i zákaznické přípojky z hlediska toků a přenášených packetů (například MRTG či obdobné), monitoring umí aktivně upozornit na vybočení sledovaných hodnot z běžného intervalu;
5. nepropaguje pomocí BGP protokolu jiné rozsahy, než ke kterým je oprávněn;
6. neposílá ze své sítě provoz z rozsahů, které nepropaguje;
7. své routery chrání v souladu s doporučením RFC6192 (control plane policy);
8. má zavedeny vnitřní procesy pro řešení incidentů;
9. zahájí práce na odstranění/omezení bezpečnostního incidentu co nejrychleji, nejpozději do 30 minut od jeho nahlášení;
10. sleduje bezpečnostní oznámení dodavatelů svých síťových komponent a patřičně na ně reaguje;
11. má všechny své weby, na kterých komunikuje se svými zákazníky či obchodními partnery, trvale přesměrovány na protokol HTTPS opatřený TLS certifikátem důvěryhodným v nejrozšířenějších webových prohlížečích, bez mixed contentu a s vypnutými šiframi, které nejsou považovány za bezpečné.
12. využívá pro jeho síť zabezpečení směrování síťového provozu technologii RPKI. Využíváním technologie RPKI se rozumí vytvoření a udržování ROA záznamů vlastněných prefixů. Ve svých vstupních filtrech má nastaveno odmítnutí nevalidních RPKI prefixů

Žadatel prohlašuje, že splňuje a po dobu členství v BV bude splňovat provozní podmínky stanovené v článku 3 Pravidel.

V \_\_\_\_\_\_\_\_, dne \_\_\_\_\_\_\_\_\_\_\_\_\_

Podpis:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_