PŘEDSTAVENÍ

NEXT GENERATION SECURITY SOLUTIONS – NESTOR

DLE RFC 2350 STANDARDU

Next Generation Security Solutions s.r.o.
U Uranie 954/18, Praha 7, 170 00
Tel.: 237 836 950
info@ngss.cz | www.ngss.cz

Identifikační údaje

Next Generation Security Solutions s.r.o.

Sídlo společnosti:	U Uranie 954/18, 170 00 Praha 7 - Holešovice
IČ:	06291031
DIČ:	CZ06291031

Společnost zapsaná v obchodním rejstříku v Praze, spisová oddíl C, vložka 279627

Webové stránky:	www.ngss.cz www.soc247.cz

Kontaktní osoby:

Radim Navrátil
Vedoucí oddělení IT Security
Tel.: +420 237 836 950
Email: rnavratil@ngss.cz

Jaromír Žák
Ředitel
Email: jzak@ngss.cz

Obsah

1. NEXT GENERATION SECURITY SOLUTIONS – NESTOR (NESTOR)

Tento dokument obsahuje popis NEXT GENERATION SECURITY SOLUTIONS NESTOR (NESTOR) týmu podle standardu RFC 2350. Poskytuje základní informace o týmu NESTOR, možnostech jeho kontaktování, jeho odpovědnosti a nabízených službách.

Datum poslední aktualizace

Toto je verze číslo 4 ze dne 1. 11. 2023.

Distribuční seznam pro oznámení

Žádný distribuční seznam pro oznámení neexistuje. Veškeré specifické dotazy nebo připomínky prosím zasílejte na adresu NESTOR.

Místa, kde může být tento dokument nalezen

Aktuální verze tohoto popisného dokumentu NESTOR je dostupná na internetových stránkách Next Generation Security Solutions s.r.o.- NESTOR (https://www.soc247.cz), kde je i ke stažení.

2. Kontaktní informace

Název týmu

NEXT GENERATION SECURITY SOLUTIONS NESTOR (zkráceně NESTOR)

Adresa

Next Generation Security Solutions s.r.o. - NESTOR

Metropolitan Building

U Uranie 954/18

170 00 Praha 7

Česká republika

Časové pásmo

SEČ, Středoevropský čas (UTC +1, od poslední neděle v říjnu do poslední neděle v březnu)

SELČ, Středoevropský letní čas (UTC +2, od poslední neděle v březnu do poslední neděle v říjnu)

Telefonní číslo

+420 237 836 950

Faxové číslo

Není k dispozici

Ostatní komunikace

Není k dispozici

Elektronická adresa

Pro hlášení incidentů prosím použijte adresu nestor@ngss.cz

Pro ostatní komunikaci prosím použijte adresu nestor@ngss.cz

Veřejné klíče a šifrovací informace

Pro hlášení incidentu i ostatní komunikaci prosím použijte tento klíč:

User ID: NESTOR <nestor@ngss.cz>

Fingerprint: 7593 D6A4 BF64 3467 22D2 8BB4 9318 D86F 1954 C4B1

PGP KeyID: 0x1954C4B1

Členové týmu

Vedoucím týmu NESTOR je Radim Navrátil. Kompletní přehled členů týmu NESTOR není veřejně k dispozici. Členové týmu se v rámci oficiální komunikace při řešení incidentu identifikují druhé straně plným jménem.

Řízení a dohled jsou zajišťovány vedoucím týmu.

Další informace

Obecné informace o NESTOR lze nalézt na stránce www.soc247.cz

Kontakt s veřejností

Preferovaný způsob kontaktování týmu NESTOR je prostřednictvím e-mailu.

Hlášení incidentů a související otázky by měly být zaslány na adresu nestor@ngss.cz. Tím se vytvoří hlášení v našem systému.

Není-li možné (nebo je-li nevhodné z bezpečnostních důvodů) použít e-mail, můžete tým NESTOR kontaktovat telefonicky.

Pracovní doba týmu NESTOR je obecně omezena na běžnou pracovní dobu (08:00-17:00 od pondělí do pátku, s výjimkou svátků).

3. Stanovy

Poslání

Tým NESTOR si klade za cíl pomáhat při ochraně informační infrastruktury svých klientů a partnerů. Naším cílem je pomoci jim účinně čelit bezpečnostním výzvám, reagovat na incidenty, koordinovat kroky k jejich řešení a účinně jim předcházet.

Cílová skupina

Naší cílovou skupinou jsou především klienti společnosti Next Generation Security Solutions s.r.o.

Zaměřujeme se na státní instituce, komerční, příspěvkové a neziskové společnosti.

Zařazení

NESTOR je součástí společnosti Next Generation Security Solutions s.r.o., která je jeho provozovatelem.

Oprávnění

NESTOR pracuje v soukromém sektoru v mezích české a evropské legislativy.

NESTOR plánuje spolupráci se správci systémů a uživateli v rámci institucí soukromého i veřejného sektoru.

4. Zásady

Typy incidentů a úroveň podpory

Tým NESTOR je oprávněn řešit všechny typy počítačových bezpečnostních incidentů, které vznikly nebo mohou potenciálně vzniknout v rámci jeho působnosti.

Úroveň podpory poskytnuté týmem NESTOR se liší v závislosti na typu a závažnosti incidentu nebo problému, velikosti uživatelské komunity a zdrojů týmu NESTOR v okamžiku incidentu, ale v každém případě bude poskytnut nějaký typ reakce během jednoho pracovního dne. Zvláštní pozornost bude věnována incidentům týkajícím se kritické informační infrastruktury.

Žádná přímá podpora nebude poskytována koncovým uživatelům. Od nich se očekává spolupráce s jejich správcem systému, správcem sítě nebo provozovatelem internetových služeb. Právě těm poskytne tým NESTOR potřebnou podporu.

Tým NESTOR se zavazuje informovat o potenciálních zranitelnostech a tam, kde je to možné, informovat výše zmíněnou cílovou skupinu o takových zranitelnostech ještě před jejich zneužitím.

Spolupráce, interakce a zpřístupňování informací

S veškerými příchozími informacemi je nakládáno bezpečně, bez ohledu na jejich závažnost. Informace, které jsou viditelně velmi citlivé povahy, budou zpracovávány a ukládány bezpečně, v případě nutnosti jsou využívány šifrovací technologie.

Tým NESTOR bude využívat informace, které mu budou poskytnuty k řešení bezpečnostních incidentů. Informace budou dále distribuovány ostatním týmům a členům pouze na základě principu need-to-know, a když to bude možné, vždy anonymně.

Tým NESTOR operuje v mezích české legislativy.

Komunikace a autentizace

Nešifrované e-maily a telefony jsou považovány za dostatečně bezpečný způsob komunikace při přenosu málo citlivých dat. Je-li nutné zaslat vysoce citlivé údaje prostřednictvím e-mailu, bude využito šifrování PGP.

Je-li nutné prověřit osobu před zahájením komunikace, může tak být provedeno buď prostřednictvím existující sítě důvěry (např. TI, FIRST) nebo jinými metodami, jako je například zpětné volání, zpětný mail nebo (v případě potřeby) osobní setkání.

5. Služby

Reakce na incidenty

Tým NESTOR si klade za cíl pomáhat místním správcům při řešení technických a organizačních aspektů incidentů. Zejména plánuje poskytovat pomoc nebo rady s ohledem na následující aspekty krizového řízení:

Třídění incidentů

- Posouzení, zda je incident věrohodný,
- Určení rozsahu incidentu a jeho priority.

Koordinace při řešení incidentu

- Kontaktování zúčastněných stran incidentu k prošetření incidentu a následné přijetí příslušných opatření,
- Usnadnění kontaktu s dalšími subjekty, které mohou pomoci s řešením incidentu,
- Informování ostatních CERT a CSIRT týmů v případě potřeby,
- Komunikace se zúčastněnými stranami a médii.

Řešení incidentu

- Poskytování poradenství o vhodných postupech lokálním bezpečnostním týmům,
- Sledování pokroku lokálních bezpečnostních týmů,
- Poskytování pomoci při shromažďování důkazů a interpretaci dat.

Kromě toho si klade tým NESTOR za cíl shromažďování statistických údajů o událostech, které se dějí v rámci jeho pole působnosti, včasné informování o možných útocích a napomáhání při ochraně proti známým útokům.

Proaktivní přístup

Tým NESTOR shromažďuje seznamy bezpečnostních kontaktů pro každou instituci v rámci svého pole působnosti. Tyto seznamy jsou k dispozici v případě potřeby při řešení bezpečnostních incidentů nebo útoků.

Tým NESTOR publikuje oznámení o závažných bezpečnostních hrozbách, aby se v nejvyšší možné míře zabraňovalo incidentům v oblasti informačních a komunikačních technologií a snížil se tak co nejvíce jejich dopad.

Tým NESTOR zpracovává IoC z dostupných zdrojů a v případě pozitivního nálezu zajišťuje předání relevantní informace kontaktu zodpovědnému za postižený systém.

Tým NESTOR se také snaží zvyšovat povědomí o bezpečnosti v rámci svého pole působnosti.

6. Formuláře pro hlášení incidentů

Formuláře pro hlášení incidentů nejsou veřejně k dispozici. Incident se nahlašuje pomocí šifrovaného mailu s využitím PGP, případně telefonicky.

Hlášení by mělo obsahovat informace:

- Kontaktní informace
- Datum a čas, kdy byl incident pozorován
- Popis události obsahující všechna relevantní data, která jsou k dispozici

7. Zproštění odpovědnosti

Navzdory všem opatřením, která budou přijata v přípravě oznámení informací, upozornění a varování, nepřebírá tým NESTOR žádnou odpovědnost za chyby, opomenutí, či škody, vyplývající z využití v nich obsažených informací.