Sdílení informací o kybernetických hrozbách

Jakub Onderka

NÚKIB

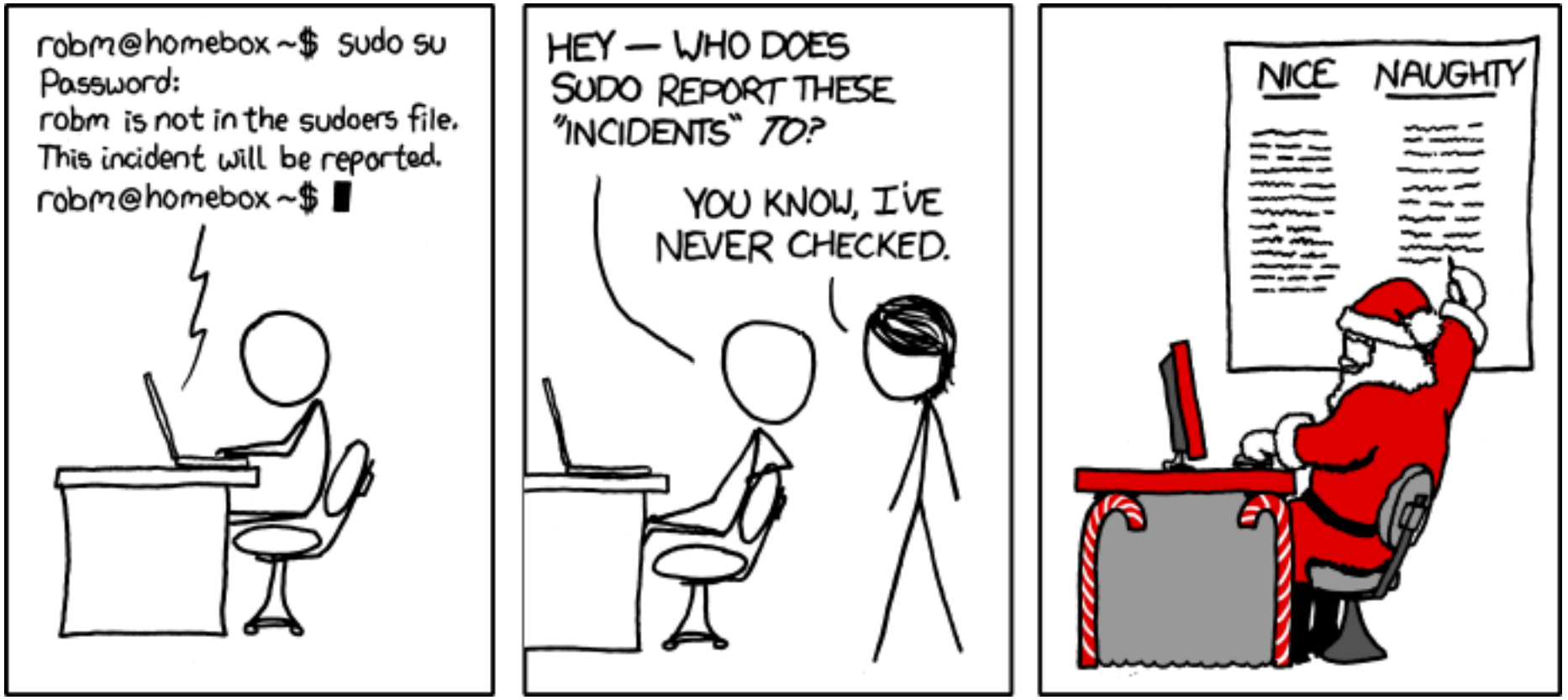
Národní úřad
pro kybernetickou
a informační
bezpečnost

Jakub Onderka

Bezpečnostní analytik, GovCERT.CZ, NÚKIB

E-mail: j.onderka@nukib.cz
Telefon: +420 720 966 958
PGP: 2EEF A5E6 CAB0 A87F 4531 1FC3 B158 F39D C523 01CD

Kybernetický bezpečnostní incident



Kybernetický bezpečnostní incident

- Organizace spadající pod zákon o kybernetické bezpečnosti mají dle současného zákona povinnost hlásit všechny kybernetické bezpečnostní incidenty na NÚKIB nebo na Národnímu CSIRT (CSIRT.CZ)

- **Kybernetický bezpečnostní incident (KBI)** = narušení bezpečnosti informací v informačních systémech
- **Bezpečnost informací** = zajištění důvěrnosti, integrity a dostupnosti informací a dat

- Hlášení KBI je hlavní zdroj informací pro NÚKIB o situaci v kybernetickém prostoru, díky němu může varovat ostatní instituce

Proč je sdílení informací důležité

CYBERSECURITY DIVE

Sign up

DIVE BRIEF

CISA's 1,200 pre-ransomware alerts saved organizations millions in damages

The federal agency's early warning system notified organizations across multiple critical infrastructure sectors of potential impending attacks.

Published Jan. 19, 2024

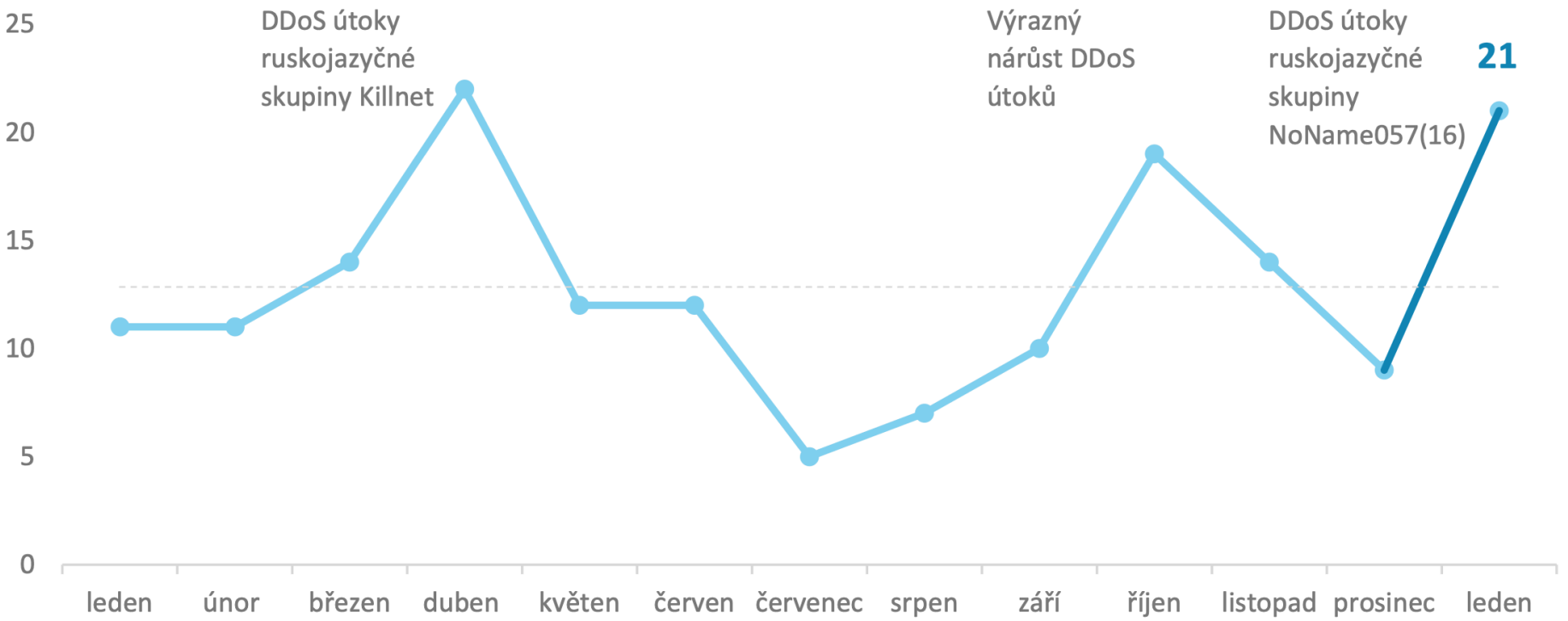
Matt Kapko
Senior Reporter

Pouze hlášení nestačí...

TLP: CLEAR

Počet kybernetických bezpečnostních incidentů nahlášených NÚKIB

V lednu NÚKIB zaznamenal více jak dvojnásobný nárůst počtu kybernetických bezpečnostních incidentů oproti předchozímu měsíci. Již první měsíc roku 2023 tak téměř dosáhl loňského maxima, jež činilo 22 incidentů za měsíc. [1]



Jak to bude s NIS2 a novým ZKB

- Dvě kategorie organizací:
  - Vyšších povinnosti – hlásí na NÚKIB
  - Nižších povinností – hlásí na Národní CSIRT

- Zásadní nárůst počtu organizací, které budou muset hlásit KBI
- Vyšší možné pokuty, takže i větší motivace organizací KBI hlásit
- Zrychlení hlášení (bezodkladně a do 24 hodin)
- Užší definice incidentů, které je třeba hlásit (pro režim vyšších povinností):
  - Pouze původ v kybernetickém prostoru
  - Pouze pokud do 24 hodin nebude možné vyloučit úmyslné zavinění

Občas mohou být KBÚ zajímavější než KBI

- **Kybernetická bezpečnostní událost** (KBU) = událost, která může způsobit narušení bezpečnosti informací

- Příklady zajímavých KBÚ:
  - Neznámý malware zachycený na AV nebo EDR na koncové stanici
  - Pokus o přihlášení s legitimním uživatelem a heslem, ale se špatným 2FA
  - Nový typ DDoS útoku, který nezpůsobil nedostupnost služby
  - Pokus o zneužití zero day, který nebyl úspěšný z důvodu hardeningu nebo jiné konfigurace

Jak sdílet informace o hrozbách

- Dle nového (ale i současného) ZKB mohou organizace hlásit i dobrovolně KBU
- NÚKIB ale do celého procesu přidává zpoždění…
- Proto chceme jít i jinou cestou a to podporou tzv. ISAC

- **ISAC = Information Sharing and Analysis Center**

- V naší představě: komunitně řízené sektorové ISAC skládající se z organizací spadající pod ZKB (banky, nemocnice, **ISP** a další)
- NÚKIB poskytne nástroje a podporu, jednotlivé organizace si ale sdílí informace mezi sebou na základě důvěry

Portál NÚKIB

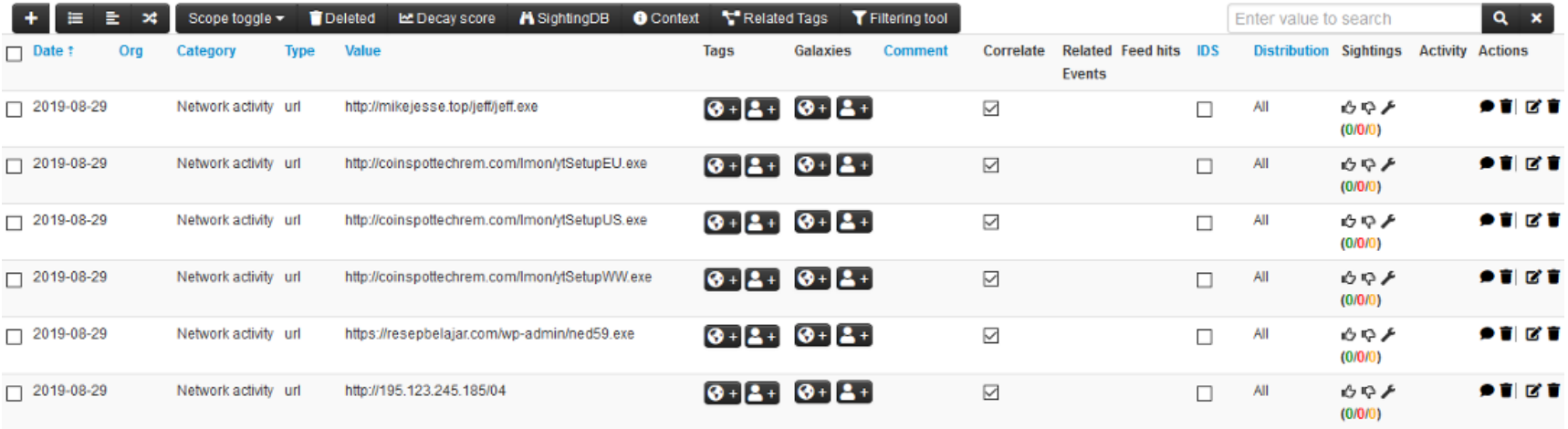
- K funkci ISAC plánujeme využít vznikající Portál NÚKIB
- Poskytne státem ověřené identity pro jednotlivé zapojené organizace
- Dva hlavní nástroje Portálu pro fungování ISAC:

MISP Threat Sharing

matrix

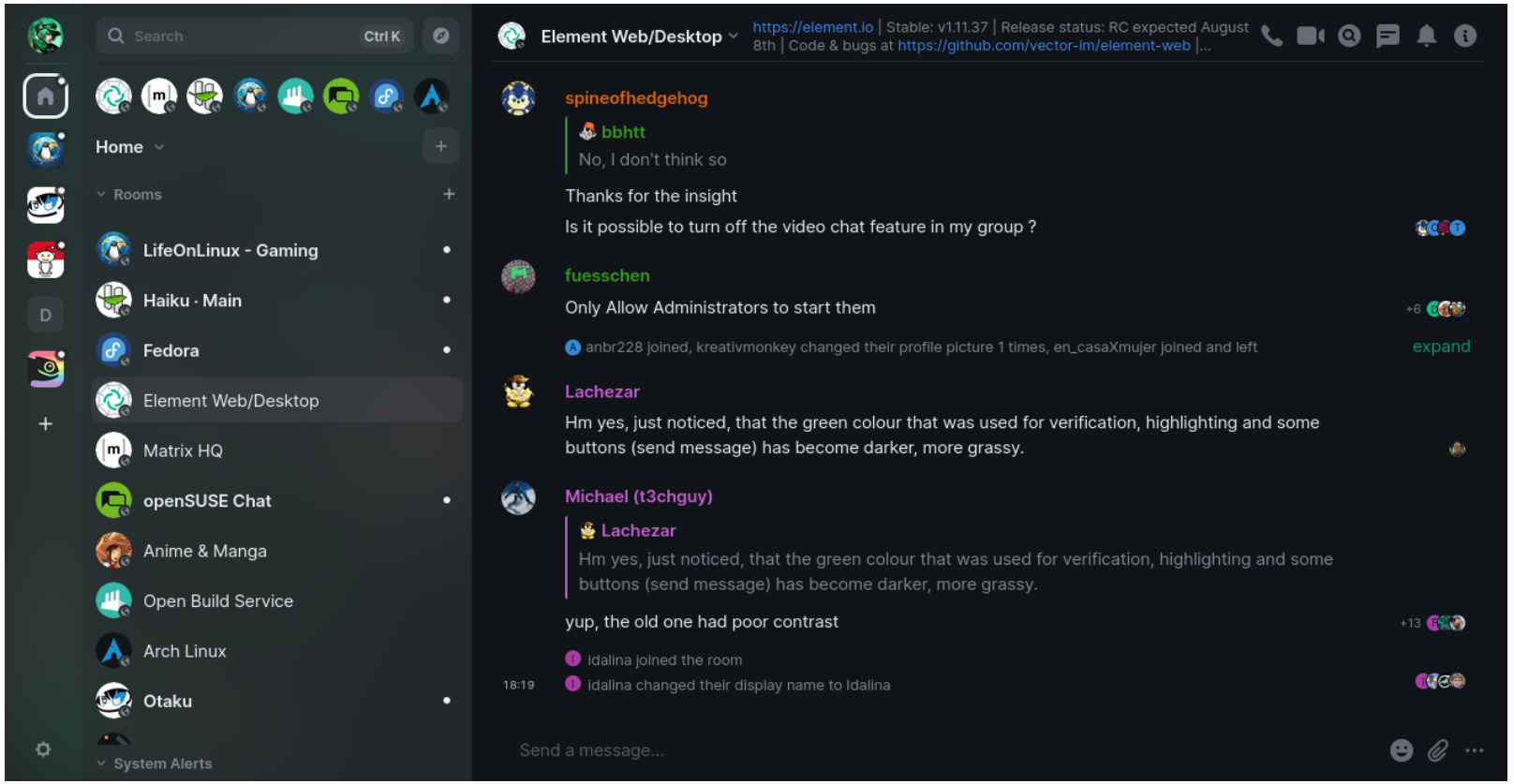
MISP - Threat sharing

- Systém pro sdílení IoC vyvíjený lucemburským CSIRT týmem
- Historicky se začal vyvíjet v NATO, později opensourcován
- NÚKIB se do vývoje zapojil, aby systém upravil pro vlastní potřeby
- Nejpoužívanější systém pro sdílení IoC v Evropě, od zpravodajských služeb, vlád po komerční společnosti
- Umožňuje sdílení jakýchkoliv indikátorů kompromitace/hrozeb (IoC) určeným skupinám



Matrix

- Open source komunikátor podporující chat, přenášení souborů nebo video i audio hovory
- Desktop a mobilní aplikace s notifikacemi



Zpětná vazba je pro nás důležitá

- Dává vám komunitně organizovaný ISAC pro sektor ISP v Česka smysl?
- Jaká organizace by měla takový ISAC zastřešovat?
- Jsou představené nástroje pro fungování ISAC dostatečné? Chybělo by vám něco?
- Sdíleli byste informace o hrozbách konkurentům?
- Preferovali byste širší nebo užší pojetí ISAC? Např. pouze pro členy FENIX?

j.onderka@nukib.cz

Jak systém MISP nasadit ve vlastní organizaci?

https://github.com/NUKIB/misp

README.md

MISP Docker image

MISP container (Docker) image focused on high performance and security based on CentOS Stream 8.

This image contains the latest version of MISP and the required dependencies. Image is intended as immutable, which means that it is not possible to update MISP from the user interface and instead, an admin should download a newer image.

Key features

- 🎩 Image is based on CentOS Stream 8, so perfectly fits your infrastructure if you use CentOS or RHEL as a host system
- ✅ Modern MISP features are enabled by default (like advanced audit log or storing setting in the database)
- 🙇 Integrated support for OpenID Connect (OIDC) authentication
- 🔒 PHP is by default protected by Snuffleupagus extensions with rules tailored to MISP
- 🚀 Optional extensions and configurations that will make MISP faster are enabled
- 📓 Integrated support for logging exceptions to Sentry and forwarding logs to syslog server
- 🧪 Final image is automatically tested, so every release should work as expected
- 🏛️ Build for amd64 (x86_64) and arm64 (aarch64)