



Kybernetická bezpečnost I

Úvod do KB a základní pojmy

Vladimír Lazecký

- ✓ **Cíl – pochopení principů KB**
 - ✓ Základní pojmy
 - ✓ Snaha o srozumitelnost
- ✓ **Motivace – proč má KB smysl**
- ✓ **Přístupy ke KB**

Když se řekne kybernetická bezpečnost

3

✓ *Co si pod tímto pojmem představíte?*

✓ *Proč má smysl KB řešit?*

✓ *Kybernetický prostor?*

✓ *Co je kybernetický incident?*

✓ *Máte zkušenost?*

- ✓ *Jak chápete pojem bezpečnost?*
- ✓ *Jaké jsou oblasti bezpečnosti?*
- ✓ *Jak jste bezpeční?*
- ✓ **Bezpečnost = značná míra nepochopení**

✓ Bezpečnost:

- ✓ Bezpečnost **není** stav systému
- ✓ Je schopnost odolávat hrozbám
- ✓ Odolnost je kvantifikována mírou
- ✓ Neexistuje „absolutní“ bezpečnost
- ✓ Míra je dána nejslabším článkem
- ✓ Mění se v čase
- ✓ Pro různé subjekty se míra liší

✓ Bezpečnost:

- ✓ Kybernetická

- ✓ Informační

- ✓ Fyzická, objektová

- ✓ Personální

- ✓ Administrativní

- ✓ Požární

- ✓ ...

✓ *Jak spolu souvisí?*

✓ Kybernetická bezpečnost (Cyber Security):

✓ *Souhrn právních, organizačních, technických a vzdělávacích prostředků směřujících k zajištění ochrany kybernetického prostoru*

Jak tomu rozumíte?

✓ **Kybernetická bezpečnost:**

- ✓ Schopnost odolávat hrozbám v kybernetickém prostoru/kybernetickým hrozbám
- ✓ Úzce souvisí s informační bezpečností
- ✓ KB je podmnožina informační bezpečnosti

✓ **Informační bezpečnost:**

- ✓ Zajištění stanovené míry dostupnosti x důvěrnosti s integritou informací
- ✓ Informační bezpečnost pokrývá nejen kybernetické hrozby
- ✓ Zmatečnost současného přístupu

Co je a není kybertická/informační bezpečnost

9

✓ Právní normy:

- ✓ NIS, NIS2
- ✓ GDPR?
- ✓ DORA?
- ✓ Občanský zákoník?
- ✓ Ochrana utajovaných informací
- ✓ Předpisy pro ISVS?
- ✓ Oborové standardy – TISAX? Standardy ve zdravotnictví?
- ✓ Co dalšího?

✓ Definice z návrhu zákona o KB (národní implementace NIS2):

- ✓ *“kybernetickým prostorem se rozumí soubor sítí elektronických komunikací a dalších technologií, ve kterém dochází ke zpracování informací a dat v elektronické podobě...”*

Jak tomu rozumíte?

- ✓ **Digitální prostor tvořený zejména globální datovou sítí**
 - ✓ Internet
 - ✓ Mobilní sítě
 - ✓ Chytrá zařízení:
 - ✓ Připojená osobní zařízení – NTB, mobily...
 - ✓ IoT, automobily, kamerové systémy
 - ✓ Cloudové služby
 - ✓ Kyber prostor není pouze surový internet
- ✓ **Jinými slovy – vše, co je digitálně propojeno a může komunikovat**



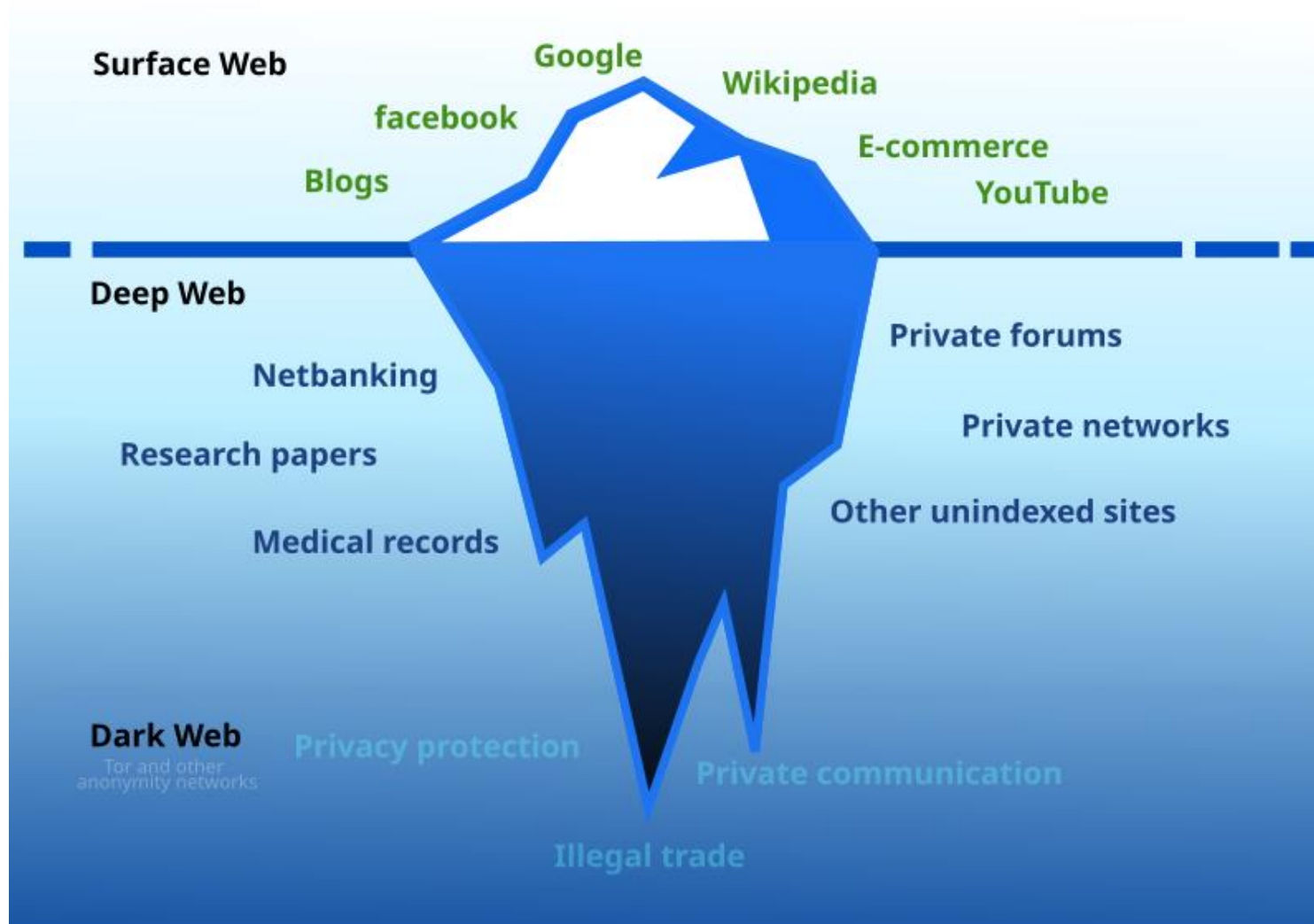
<https://czechsmartcitycluster.com/>

✓ Je součástí kyber prostoru:

- ✓ Standalone stanice?
- ✓ IT administrátor
- ✓ Asistentka
- ✓ Vendor?
- ✓ Serverovna?

Kyber prostor - struktura webu

14



https://commons.wikimedia.org/wiki/File:Iceberg_of_Webs.svg

✓ Vlastnosti důležité pro bezpečnost

- ✓ Svět bez limitů
- ✓ Svět víry
- ✓ Trvalá digitální stopa
- ✓ Deanonymizace uživatele x anonymita útočníků
- ✓ Retrospektiva
- ✓ Větší digitalizace lidských životů
- ✓ Evoluce nám nedala šanci

✓ Bude v samostatných přednáškách

[NÚKIB](#) > [Infoservis](#) > [Aktuality](#) > Software i hardware společností Huawei a ZTE je bezpečnostní hrozbou

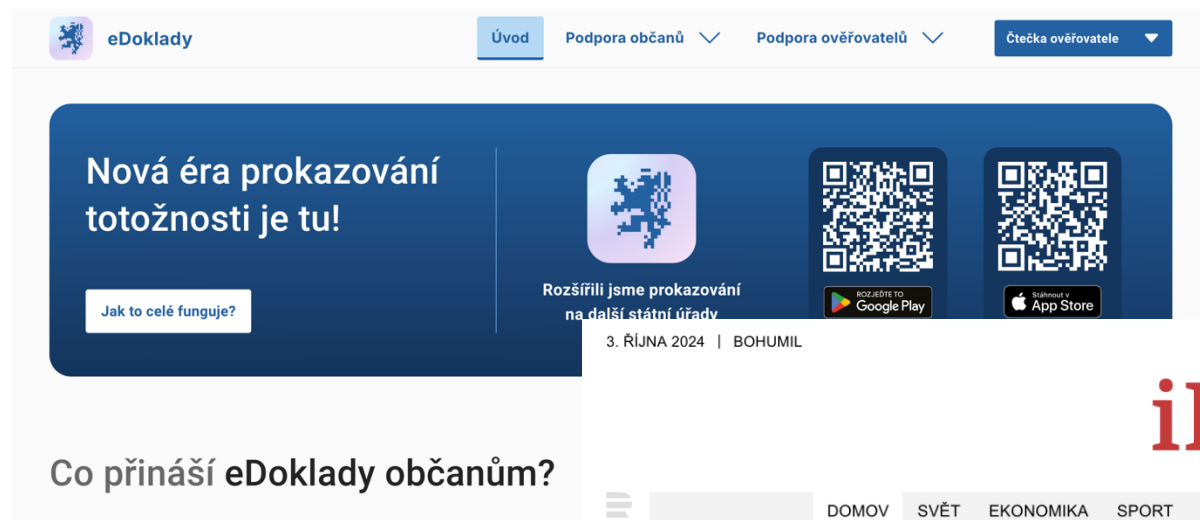
Software i hardware společností Huawei a ZTE je bezpečnostní hrozbou

17. prosinec 2018

Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) vydal VAROVÁNÍ před používáním softwaru i hardwaru společností Huawei Technologies Co., Ltd., a ZTE Corporation. Používání těchto prostředků představuje bezpečnostní hrozbu.

„K vydání tohoto varování nás vedly naše poznatky včetně poznatků z činnosti našich bezpečnostních partnerů a také zjištění našich spojenců. Hlavním problémem je právní a politické prostředí Čínské lidové republiky, ve kterém uvedené společnosti primárně působí. Čínské zákony vyžadují po soukromých společnostech působících v Číně mimo jiné součinnost při zpravodajských aktivitách, a tudíž pouštět je do systémů, které jsou klíčové pro chod státu, může představovat hrozbu,“ říká ředitel NÚKIB Dušan Navrátil.

<https://nukib.gov.cz/cs/infoservis/aktuality/1303-software-i-hardware-spolecnosti-huawei-a-zte-je-bezpecnostni-hrozbou/>



iROZHLAS

Kde se nacházíte: [iROZHLAS.cz](https://www.irozhlas.cz) / [Zprávy z domova](#) | Související témata: [edoklady](#) [eObčanka](#) [soukromí](#) [sledování](#) [DIA](#) [NAKIT](#) [Ivan Bartoš](#) [digitalizace](#) [eGovernment](#)

Digiobčanka má chránit soukromí, přitom hlásí, kdo se kde ověřuje. ‚Sběr dat omezíme,‘ slibuje agentura

https://www.irozhlas.cz/zpravy-domov/eobcanka-edoklady-egovernment_2407260620_cib

Retrospektivní hrozby

HOSPODÁŘSKÉ NOVINY

BYZNYS ZPRÁVY NÁZORY TECH REALITY INVESTICE PODCASTY PročNe ARCHIV DALŠÍ



Každý systém je napadnutelný. Největší riziko si ale působí uživatel sám, říká bezpečnostní expert Lazecký

Problém uživatelů je ten, že moc nechápu principy, jak internet, e-mail nebo sociální sítě fungují, říká bezpečnostní expert Vladimír Lazecký....

30. 9. 2015 • 1 min. čtení



Palec nahoru pro Zuckerberga. Na Facebook se poprvé během jednoho dne připojila sedmina obyvatelstva Země

Do největší sociální sítě Facebook se během jednoho dne historicky poprvé připojila více než miliarda uživatelů, tedy přibližně sedmina...

28. 8. 2015 • 1 min. čtení

<https://hn.cz/tagy/uzivatele-13505>



Kompletní spis spolupracovníka StB Andreje Babiše

8

SEZNAM DOKUMENTŮ
ve věci — spis registrační číslo — 58-101-1

Pol. číslo	Označení dokumentu (číslo, datum, obsah)	Platnost (datum, místo)	Podpis
16	Učební na samostatné uč. 26	24-25	
17	Učební na 76	24	
18	Každen z prvních	25-26	
19	Začíná a vypracuje by	22	
20	20. a 21. 10. 1989	20	
21	Výsledky 76	27-30	Emil
22	Contr. 674	31	21. 10. 1989
23	TI - výsledky	32	21. 10. 1989
24	Vnímání na uč. 106	33	
25	TI - výsledky	34	
26	Každen z uč. 106	35-36	
27	Výsledky	37-39	
28	Učební na prvních	40-41	
29	Začíná a vypracuje	42	
30	Učební na D	43	

MY 8. 08. 723

Foto: Aktuálně.cz

<https://zpravy.aktualne.cz/domaci/kompletni-spis-spolupracovnika-stb-andreje-babise/r~i:gallery:31547/r~i:photo:571925/>

✓ Ochrana hodnot

- ✓ *Co je bezcenné nemá smysl chránit*
- ✓ *Výše hodnoty je zásadní vodítko pro bezpečnost*

- ✓ Zákonné a regulatorní požadavky
- ✓ Obava z pokud
- ✓ Požadavky trhu
- ✓ Společenská odpovědnost

- ✓ *Daty se rozumí záznamy jednání, skutečností nebo informací a soubory takových jednání, skutečností nebo informací, včetně provozních údajů) a metadat), zejména v podobě textu, čísel, grafů, obrazů, zvuku a videa*
- ✓ *Informací jsou zpracovaná, interpretovaná nebo uspořádaná data, která mají význam a kontext,*

Jak tomu rozumíte?

✓ Informace:

- ✓ Existuje mnoho definic
- ✓ Sdělitelný poznatek, který má smysl a snižuje neznalost
- ✓ Informační šum, fake news...
- ✓ Pojem informace je nutno chápat obecně – ne pouze data v elektronické podobě
- ✓ Jednotka informace – 1 bit – víte, co znamená?

✓ Data:

✓ Zaznamenané informace schopné přenosu, uchování, interpretace, zpracování

✓ Forma:

- ✓ Elektronická
- ✓ Hlasová
- ✓ Fyzický záznam

✓ Data jsou spojena s nosičem dat:

- ✓ Kamenná deska
- ✓ Elektronická média
- ✓ Papír
- ✓ Mozek

✓ Zajištění důvěrnosti, dostupnosti a integrity:

✓ **Důvěrnost** – k informaci má přístup pouze ten, kdo je k tomu oprávněn

✓ **Dostupnost** – informace je dostupná v čase, kdy je potřeba

✓ **Integrita** – informace u zdroje a cíle je identická:

✓ Odolnost proto neoprávněné změně

✓ Úplnost

✓ Korektnost kontextu:

✓ Integrita databáze bez osiřelých dat

✓ Integrita generuje největší problém pochopení

✓ Hodnota:

- ✓ Informace mají hodnotu
- ✓ Hodnota se pro jednotlivé subjekty liší
- ✓ Hodnota se může extrémně rychle měnit v čase
- ✓ *Jak stanovíte hodnotu informace?*

✓ Obtížná detekovatelnost:

✓ Zaručení integrity:

- ✓ Detekovatelnost změny, úplnosti
- ✓ Ověření autenticity – pravdivosti, hodnověrnosti

✓ Zaručení dostupnosti:

- ✓ Detekovatelnost ztráty
- ✓ Jak detekovat ztrátu, když o informaci nevím?

✓ Zaručení důvěrnosti:

- ✓ Jak detekovat prozrazení informace?

✓ Zajištění důvěrnosti, dostupnosti a integrity:

- ✓ V celém životním cyklu informací

- ✓ Během jejich vzniku, zpracování, ukládání, přenosu a likvidace

- ✓ Informační systém?

- ✓ Využitím logických, technických, fyzických a organizačních opatření

- ✓ Opatření musí pokrývat všechny identifikovatelné hrozby s vyšší mírou rizika

- ✓ **Důvodem pro bezpečnost je hodnota**
- ✓ Bezpečnost => kompromis mezi
 - ✓ Mírou bezpečnosti
 - ✓ Komfortem
 - ✓ Náklady
- ✓ **Hledání optima => neexistuje systém tří maxim**

✓ Bezpečnost je komplikace s nemalými náklady

- ✓ Bezpečnost se neřeší
- ✓ Vědomé rozhodnutí k přijetí škod
- ✓ Přijetí zodpovědnosti za škody

✓ Ad Hoc bezpečnost

- ✓ Bezpečnost se řeší ad Hoc
- ✓ Bez hlubšího porozumění
- ✓ Neefektivně vynaložené náklady
- ✓ Nepokrytí hrozeb s vyšší mírou rizika
- ✓ Falešný pocit bezpečí

✓ Systematický proces

✓ Pochopení principů

✓ Systematický a nikdy nekončící proces založený na managementu rizik

✓ Optimalizace nákladů vzhledem k hodnotám a výši škod

✓ Ani zde neexistuje absolutní bezpečnost

✓ Hrozbou se rozumí:

- ✓ Jakákoliv potenciální okolnost, událost nebo jednání, které mohou být příčinou kybernetické bezpečnostní události nebo kybernetického bezpečnostního incidentu, a která mohou poškodit, narušit nebo jinak nepříznivě ovlivnit aktiva, jejich uživatele nebo další osoby

✓ Lidsky – to, co mne ohrožuje

- ✓ Ztráta mobilu
 - ✓ Dopad – nedovolá se mi klient, přijdu o business

- ✓ Kybernetickou bezpečnostní událostí je událost, která může vyústit v kybernetický bezpečnostní incident
- ✓ Kybernetickým bezpečnostním incidentem je narušení bezpečnosti informací v kybernetickém prostoru

✓ Prolomení důvěrnosti x dostupnosti x integrity

- ✓ Kyber útoky – ransomware, dDOS...

- ✓ Technická selhání

- ✓ Lidské chyby a selhání

- ✓ Využití příležitosti

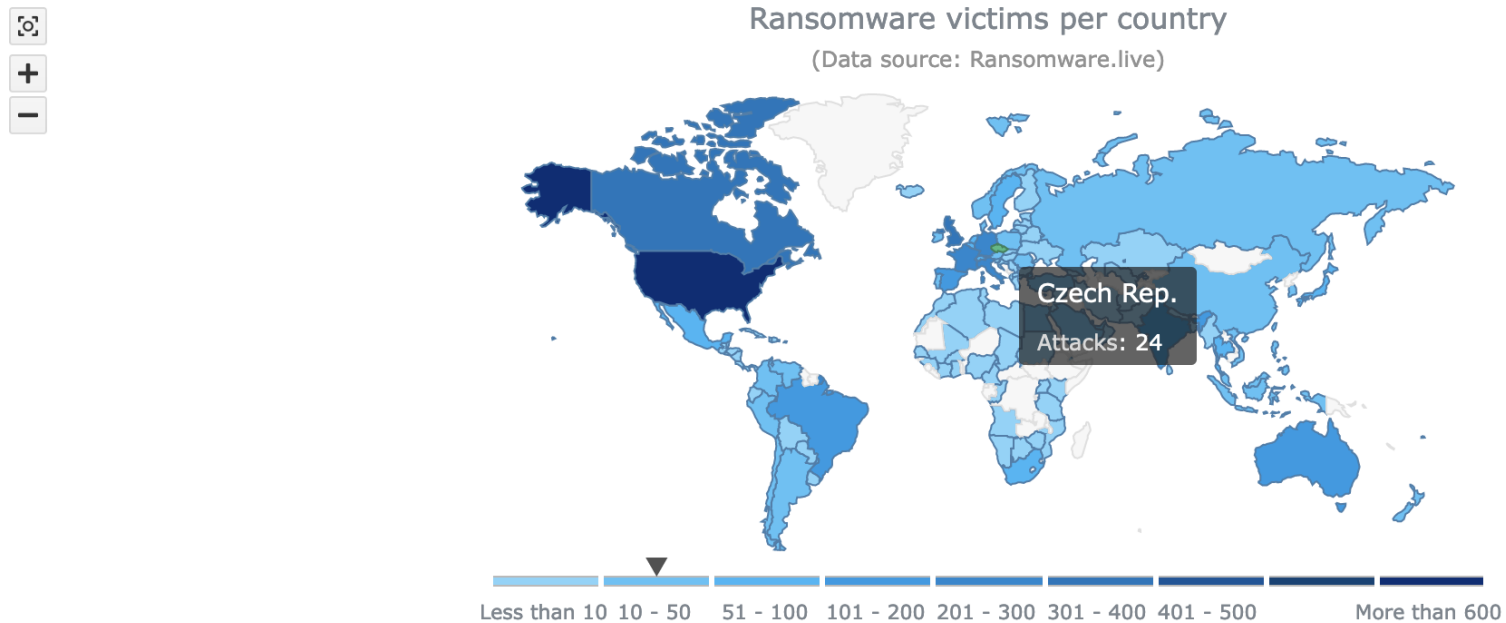
✓ Nejen v kybernetickém prostoru

✓ *Jak je účinné strašení útoky?*

Útoky za poslední rok v ČR – zdroj Darknet

34

Ransomware WorldMap



<https://www.ransomware.live/map/>

Útoky v ČR – zdroj Darknet

35



The screenshot shows a web browser window with the URL <https://www.ransomware.live/map/CZ>. The page title is "24 Ransomware victims from Czechia". A sidebar on the left contains a search bar and a menu with the following items: Recent victims, Cyberattacks in the press, Ransomware Groups, Negotiation Chats, Ransom Notes, Statistics, Victims by country, Cartography, and Tools Matrix. The main content area features a sponsored message from Hudson Rock, a list of statistics for Czechia (Region: Europe, Capital: Prague, Population: 10,521,600, 71 CERTs/CSIRTs found), and a green box stating that the page lists all victims of ransomware attacks in the Ransomware.live database for Czechia. Below this, the heading "Top 10 Ransomware Groups in Czechia" is visible.

← → ↻ 🔍 📄 https://www.ransomware.live/map/CZ 📄 ★ 🛡️ 🔊 ☰

24 Ransomware victims from Czechia ?

Sponsored by **Hudson Rock** – [Use Hudson Rock's free cybercrime intelligence tools to learn how Infostealer infections are impacting your business](#) ↗

🌐 Region: Europe
🏙️ Capital: Prague
👥 Population: 10,521,600
🛡️ 71 CERTs/CSIRTs found 🇸🇰

This page lists all the victims of ransomware attacks in **Ransomware.live** database for Czechia. We continuously scrape ransomware group site to detect new victims.

Top 10 Ransomware Groups in Czechia

<https://www.ransomware.live/map/>

[Main](#)[About](#)[Rules](#)[Partners](#)[FAQ](#)

Below is a list of companies that either have considered their financial gain to be above the interests of their partners / individuals who have entrusted their data to them or have chosen to conceal the fact that they have been compromised.

HOT NEWS Lake Washington Institi



[\[redacted\].cz/en/](#)

👁 9310 Status: EVIDENCE Action: Encrypted Action date: 18/08/2024

[DISCLOSED][TORRENT] Roberto Verino Difusion

<https://www.robertoverino.com/>

👁 9085 Status: DISCLOSED Action: Encrypted Action date: 04/05/2023

Jeden ze seznamu linků - ransomware

37

ransomwr3tsydeii4q43vazm7wofla5ujdajquitomtd47cxjtfgwyd.onion

Ransomware Group Sites

If you want to buy me a coffee for my work, donations are warm welcome to one of those addresses:
DOGE: DBPbrvFShnykgBa8svQ91F9Vgs1zhgmB1
LTC: LXMdZiBcT474Mava74r9BvkTyoxcaUk6MD
BTC/BCH: 1FyCD8kp9ekiTTgdyhFtZRgzR1QCHV4i84
XMR: 48FgeW4fUpyjPDGxJdHaA441F5c9szYtLSVWbNv8T3Zxe9ZN3iLUSSdASof2vDQqdbgRYom9aMeQMWPQkr3SPZUJE2uM8fc

Group Name	Onion V.	Link
Arvin Club	v3	Open
Babuk	v3	Open
Black Basta	v3	Open
AlphaVM/BlackCat	v3	Open
BlackByte	v3	Open
Bl4ckt0r	v3	Open
CL0P	v3	Open
CONTI	v3	Open
CRYP70N1C0D3	v3	Open
Cuba	v3	Open
Everest	v3	Open
Grief	v3	Open
Hive	v3	Open
HolyGhost	v3	Open
Karakurt	v3	Open DEEP-WEB
KelvinSecurity		DEEP-WEB
LockBit 2.0	v3	Open
LockData Auction	v3	Open
Lorenz	v3	Open
LV BLOG	v3	Open Open
Medusa	v3	Open
Midas	v3	Open
Moses Staff	v2	Open DEEP-WEB
Pandora	v3	Open
Pay2Key	v3	Open
Quantum	v3	Open
Ragnar_Locker	v3	Open

✓ Bude samostatné téma

Aktivem je fyzický nebo digitální prostředek, osoba nebo činnost související se zpracováváním informací a dat v elektronické podobě.

- ✓ Definice aktiv je mírně zavádějící
- ✓ V různých standardech a regulativech se liší => **generuje značné problémy**

✓ Aktivum = vše, co má hodnotu

- ✓ Reputace
- ✓ Know how
- ✓ Informace
- ✓ Zaměstnanci
- ✓ Business aktivita
- ✓ Soukromí
- ✓ Výrobní systémy
- ✓ IT systémy...

✓ Primárním aktivem je aktivum v podobě zpracovávané informace nebo poskytované služby

✓ Nešťastná definice – služba nebo informace?

- ✓ **Informace, nebo služba, kterou poskytuje informační systém**
 - ✓ Výrobní proces – je řízen IT systémem
 - ✓ Informace o nákladech pro sestavení nabídky – sestava z IT systémů
 - ✓ Business aktivita postavená na IT systému

- ✓ **Odhad ceny:**
 - ✓ Jaká mi vznikne škoda u nedostupnosti aktiva

- ✓ Podpůrným aktivem je aktivum zajišťující fungování primárních aktiv, zejména zaměstnanec, dodavatel, technické aktivum, budova a jiný ohraničený prostor, ve kterém se nachází aktivum regulované služby
- ✓ Technickým aktivem je technický nebo programový prostředek anebo vybavení.

✓ Vše, na čem je závislé primární aktivum

- ✓ IT systémy
- ✓ Data
- ✓ Objekty
- ✓ Lidé
- ✓ Dodavatelé

- ✓ **Business aktivum** – obchodní činnost, aktivita, obvykle generuje profit
- ✓ **Informační aktivum** – informace, které mají hodnotu, tedy má smysl je chránit
- ✓ Nešťastné matení pojmů (ISO 27000, SOC2, NIS2, DORA, TISAX...)

✓ Organizační opatření:

- ✓ Systém řízení bezpečnosti informací (ISMS)
- ✓ Požadavky na vrcholné vedení
- ✓ Stanovení bezpečnostních rolí
- ✓ Řízení bezpečnostní politiky a bezpečnostní dokumentace
- ✓ Řízení aktiv
- ✓ Řízení rizik
- ✓ Řízení dodavatelů
- ✓ Bezpečnost lidských zdrojů
- ✓ Řízení změn

✓ Organizační opatření:

- ✓ Akvizice, vývoj a údržba
- ✓ Řízení přístupu
- ✓ Zvládání kybernetických bezpečnostních událostí a incidentů
- ✓ Řízení kontinuity činností
- ✓ Provádění auditu kybernetické bezpečnosti

✓ Technická opatření:

- ✓ Fyzická bezpečnost
- ✓ Bezpečnost komunikačních sítí
- ✓ Správa a ověřování identit
- ✓ Řízení přístupových práv a oprávnění
- ✓ Detekce kybernetických bezpečnostních událostí
- ✓ Zaznamenávání událostí
- ✓ Vyhodnocování kybernetických bezpečnostních událostí
- ✓ Aplikační bezpečnost
- ✓ Kryptografické algoritmy
- ✓ Zajišťování dostupnosti regulované služby
- ✓ Zabezpečení průmyslových, řídicích a obdobných specifických technických aktiv

- ✓ **Bezpečnost není stav**
 - ✓ Systematické, důsledné a trvalé snižování rizik
- ✓ **Pochopení základních pojmů**
- ✓ **Příště – standardy a regulace**
 - ✓ Aneb proč vymýšlet vymyšlené...
- ✓ **Bezpečnost není romantika, ale tvrdá dřina 😊**

Prostor pro vaše dotazy...

Děkujeme za pozornost

Za tým VIAVIS a.s.

- Vladimír Lazecký