



CyberSec Forum Praha 2023

Jsou důvodem, proč se zabývat NIS 2, drakonické pokuty?

Vladimír Lazecký

vladimir.lazecky@viavis.cz

Portfolio služeb VIAVIS a.s.

Poskytujeme expertní služby v oblasti kybernetické, informační a fyzické bezpečnosti včetně penetračního testování, poradenství, vzdělávání, řešení incidentů a znaleckých posudků.



Penetrační
testování



Ochrana
měkkých cílů



GDPR



Bezpečnost



Vzdělávání



Řešení
bezpečnostních
incidentů



Outsourcing



Poradenství



Posudky



Bezplatné online
workshopy

...již více jak 20 let střežíme podstatné

- ✓ Co je NIS 2:
 - ✓ Stav, legislativní proces
- ✓ Kdo pod NIS 2 spadá:
 - ✓ Režim vyšších a nižších povinností
- ✓ Povinnosti ukládané NIS 2
- ✓ Drakonické pokuty
 - ✓ Obdoba s GDPR

The NIS2 Directive

A high common level of cybersecurity in the EU

OVERVIEW

The Network and Information Security (NIS) Directive is the first piece of EU-wide legislation on cybersecurity, and its specific aim was to achieve a high common level of cybersecurity across the Member States. While it increased the Member States' cybersecurity capabilities, its implementation proved difficult, resulting in fragmentation at different levels across the internal market.

[https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI\(2021\)689333_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf)

Jiný pohled – je NIS 2 důvod, proč IKB řešit?

4 / 14

- ✓ **Ano je, ale neměl by být důvodem primárním**
- ✓ **Důvodem pro IKB by neměly být drakonické pokuty**
- ✓ **Důvodem pro KB je ochrana hodnot –aktiv**
- ✓ **Efektivnost opatření (risk management je základem)**

The screenshot shows the AvosLocker ransomware payment interface. At the top, it says "Payment" and "AvosLocker" with a logo, and "English" in the top right corner. Below this, there are three main sections:

- Before deadline:** Shows payment options: \$200,000.00 USD, 800.00 XMR, and 4.17 BTC (25% processing fee).
- Deadline:** Shows the date and time: "Date: Mon, 19 Sep 2022 13:58:57 GMT" and "Time left: 4 days 23 hours 59 minutes".
- Past deadline:** Shows payment options: \$400,000.00 USD, 1600.00 XMR, and 8.34 BTC (25% processing fee).

Below these sections, there is a "Test decryption" section with instructions: "You may test our decryption process by uploading a single encrypted image file (PNG, JPG, JPEG, GIF, TIFF, BMP) less than 1 MB in size." It includes a "Browse..." button, a "Decrypt" button, and a message "No file selected.".

On the right side, there is a "Support" chat window with a "Refresh" button. The chat message from "Staff" says: "As you are an enterprise client of ours, we will provide you with customer support throughout the process. You may use this chat to get in contact with us." At the bottom of the chat window, there is an input field "Enter your message" and a "Send" button.

Jaká je šance, že budu obětí útoku?

5 / 14

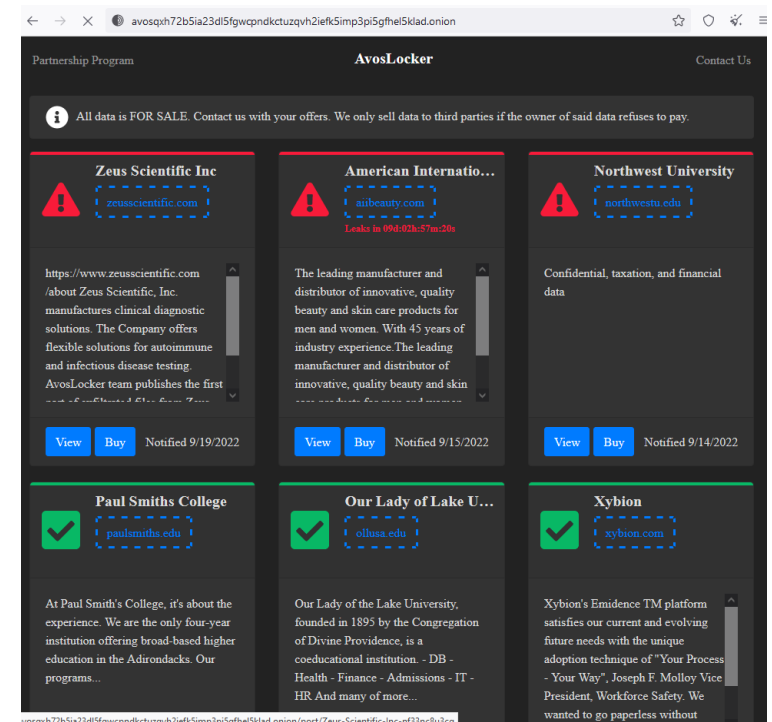
✓ Nejsem zajímavý, kdo by na mne útočil

- ✓ Příklady z prezentací – strašení velkými útoky
- ✓ V IS neprovozují nic zajímavého
- ✓ Vždyť školím uživatele o phishingu

The screenshot shows a ransomware website with a logo 'AVANTON RANSOMWARE' in the top left. The page is divided into three main sections:

- New companies:** A list of companies with their names, next update times, and a red 'DDOS' button. The companies listed are FEBANCOLOMBIA, Cube Audit Ltd, Halwani Bros Ltd, Rate Rabbit Inc, JetSJ, Maryan beachwear group GmbH, and 360 InStore.
- Company details:** A central section showing details for a specific company, with most information redacted by black boxes. Visible fields include Company, Address (Czech Republic), Website, Email, Phone, and Files (a list of zip files with sizes).
- Full dumps:** A list of companies with their names and published data sizes. The companies listed are TAIWAN SURFACE MOUNTING TECHNOLOGY CORP., Cinov Federation, Glasbau Wiedemann GmbH, Cocal, SPINE & DISC, EUROMAIS - PEÇAS E PNEUS, LDA, and Schepis Communications.

- ✓ Oběti si útok samy přivolaly – komunikují zranitelnosti
- ✓ Útoky jsou business – útočníkům je jedno, kdo obětí je
- ✓ K naplánování a provedení stačí motivace a základní znalosti
- ✓ Důvodem pro KB není ani právní úprava, ani pokuty, ale ochrana hodnot



Kde získat ransomware a naučit se jej používat

RANION - Better & Cheapest FUD Ransomware + Darknet C2 + NO Fees

BUY - FAQ - REVIEWS - SCREENS - CONTACT

*We provide an already configured and compiled FUD Ransomware + Decrypter
We are the only that provide a FREE Anonymous C2 Dashboard via Onion to manage your Clients
We also provide additional FREE Customizations and take NO FEES from your Clients*

**DISCLAIMER: Our Products are for EDUCATIONAL PURPOSES ONLY.
Don't use them for illegal activities. You are the only responsible for your actions!
Our Products/Services are sold with NO WARRANTY and AS ARE.**

***** THE ONLY ORIGINAL ONE (v3): <http://jt4tpffl mrb7jfpk6jcw xewqmmzids4syg4sjyecqhdj2oc43ib3adid.onion> *****

Version: 2.30

-= NEWS =-

- 2022/11 : RANION v1.85 released (re-FUD)
- 2023/2 : RANION v2.00 released (re-FUD)
- 2023/4 : RANION v2.15 released (re-FUD)
- 2023/7 : RANION v2.30 released (re-FUD)

<http://jt4tpffl mrb7jfpk6jcw xewqmmzids4syg4sjyecqhdj2oc43ib3adid.onion/>

Změna ve způsobech vydírání

8 / 14

Enter UUID

Feedback

Public notice



TOP

snatch

New company

Full data

Archive

Search for company...

Insurance companies, attention please!

- In case you see your client in this list, please contact us. You will get a full access gaining report of the company. This will totally convince you that the poor judgment of the IT department leads to an insured event. Since many companies have turned attacks on them into a profitable insurance business, we are starting to publish reports on breaches in the security systems of those who are mentioned at our blog.

Your presence at this page means that we obtain your sensitive information and in case of your silence and refuse to bear responsibility this data will be published no matter how important and confidential

New

Aug 21, 2023 09:50 PM

2286

Department of Defence South African (DARPA)

1.6 TB

Military contracts, internal call signs and personal data

Read more



New Company

Department of Defence South African (DARPA)

Military contracts, internal call signs and personal data

leakage:

...

Gemma Bignell:CFO, Director, Operations, Financial Officer

gemma.bignell@briarsgroup.com;

Andrew Brierley:Chairman

andrew.brierley@briarsgroup.com;

Emma Lisauskas:Director, Director, Operations

emma.lisauskas@briarsgroup.com;

<http://hl66646wtlp2naoqnhattngigjp5palgqmbwixepcjyq5i534acgqyad.onion/index.php>

✓ Jak řešit informační a kybernetickou bezpečnost:

- ✓ Systematicky, důsledně, efektivně
- ✓ Přístup založený na managementu rizik

✓ Systematické kroky:

- ✓ Management rizik
- ✓ Organizační opatření
- ✓ Technická opatření

✓ *Jakou vidíte nevýhodu?*

- ✓ **Kroky ke snížení největších rizik**

- ✓ Paralelně se zahájením systematických kroků:
 - ✓ **Přesvědčit management**
 - ✓ **Zálohování, BCP, DRP**
 - ✓ Zálohy 3x2x1 – pozor na cloudové zálohy
 - ✓ Retence
 - ✓ Testy, testy, testy

- ✓ **Zabezpečení perimetru, prostupy**

✓ OSINT – Open Source Intelligence

- ✓ Získávání informací z veřejných zdrojů
- ✓ Legální, neinvazivní, nedetekovatelný
- ✓ Útočníci využívají OSINT pro vyhledání obětí

✓ Pravidelný OSINT je nedílnou součástí bezpečnostních procesů

- ✓ Vědět, co se o mně ví
- ✓ Odstranění, potlačení rizikových informací

✓ *Kdo si dělá OSINT na sebe, organizaci?*

✓ NIS 2 je příležitost

- ✓ Důvodem je ochrana hodnot
- ✓ Bezpečnost systematicky, důsledně
- ✓ Argument pro manažery
- ✓ Dělejte si OSINT

Nadcházející workshopy

KYBER ČTVRTEK

Jak vzdělávat zaměstnance?

Termín: 7. 9. 2023

Čas: 9:30 - 10:15h

[Zjistit více](#)

KYBER ČTVRTEK

Jak vzdělávat management?

Termín: 21. 9. 2023

Čas: 9:30 - 10:15 hodin

[Zjistit více](#)

MIMOŘÁDNÉ WORKSHOPY

Analýza k posouzení vlivu (Úterý s pověřencem č. IV/2023)

Termín: 26. 9. 2023

Čas: 9:30 - 11:30 hodin

[Zjistit více](#)



Pravidelně, online a bezplatně



Proč nás sledovat



Technické požadavky

Prostor pro vaše dotazy...

Děkujeme za pozornost

Za tým VIAVIS a.s.

- Vladimír Lazecký