



Zabezpečení dat i s nízkým rozpočtem

26.10.2023





Kdo jsem?

Kdo jsem?

Jakub Alimov, CEH, CHFI



Lead Auditor

architekt kybernetické bezpečnosti,
RANSOMWARE hunter,

konzultant informační bezpečnosti,

více jak 13+ let prokazatelných zkušeností s
kybernetickou bezpečností


<https://www.linkedin.com/in/jakub-alimov-332b1020/>



Kdo je Alinet?



Jsme progresivní IT firma se specializací na kybernetické útoky.



DIGITAL FORENSICS AND INCIDENT RESPONSE

SLUŽBY KYBERNETICKÉ BEZPEČNOSTI

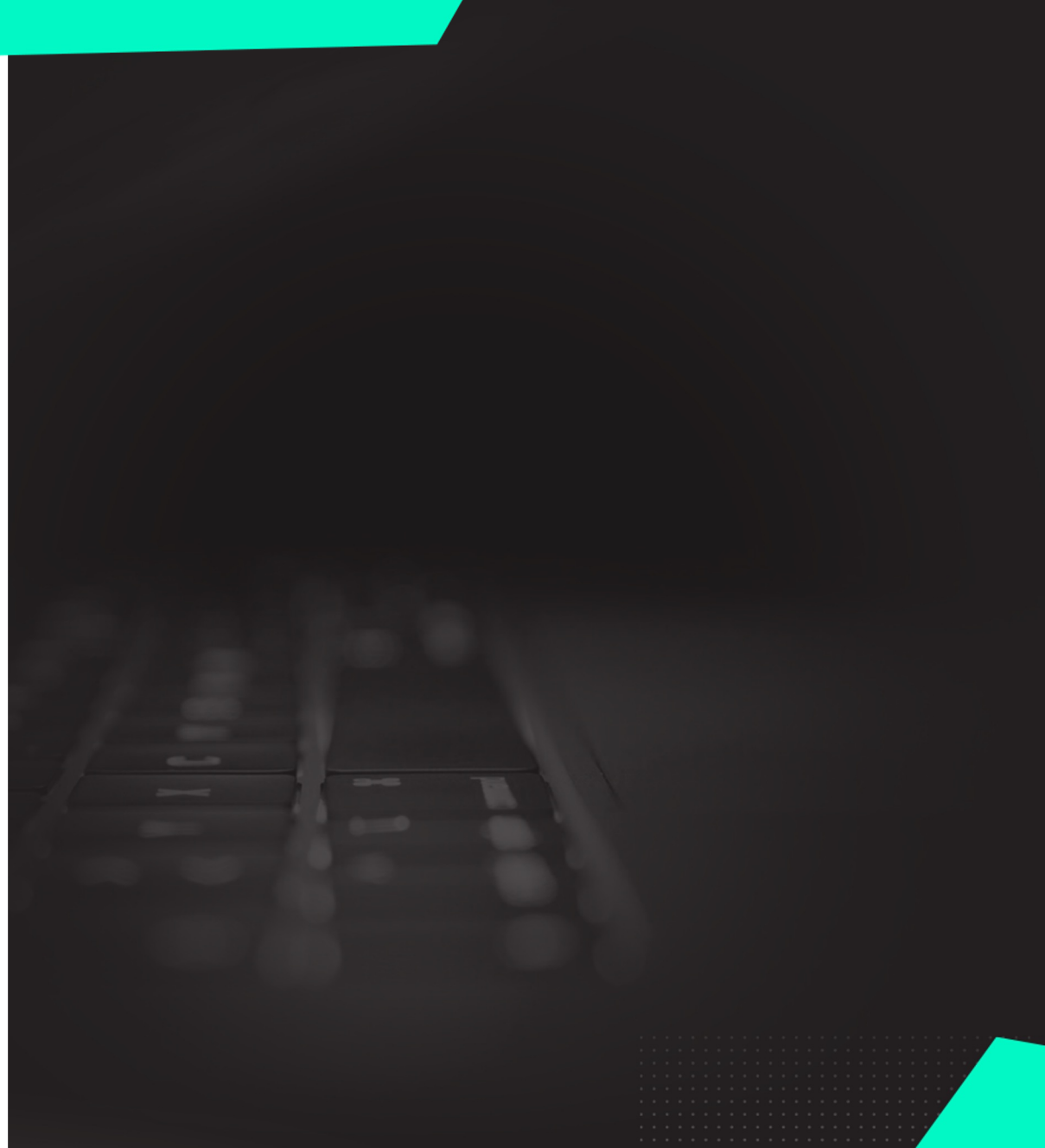
SLUŽBY DETEKCE KYBERNETICKÝCH UDÁLOSTÍ



Co se děje a jak je to vůbec možné?

Co se děje a jak je to vůbec možné?

**Chtěl bych se s Vámi podělit o několik
skutečných příběhů z forenzního
vyšetřování.**



Co se děje a jak je to vůbec možné?

**Chtěl bych se s Vámi podělit o několik
skutečných příběhů z forenzního
vyšetřování.**

- ✓ **Uživatel klikne na nevhodný e-mail a zašifruje
celou firmu**

Co se děje a jak je to vůbec možné?

Chtěl bych se s Vámi podělit o několik skutečných příběhů z forenzního vyšetřování.

- ✓ Uživatel klikne na nevhodný e-mail a zašifruje celou firmu
- ✓ Někdo otevře infikovaný soubor s malware a způsobí nedostupnost systémů

Co se děje a jak je to vůbec možné?

Chtěl bych se s Vámi podělit o několik skutečných příběhů z forenzního vyšetřování.

- ✓ **Uživatel klikne na nevhodný e-mail a zašifruje celou firmu**
- ✓ **Někdo otevře infikovaný soubor s malware a způsobí nedostupnost systémů**
- ✓ **Nepoužívání MFA na VPN s kombinací zneužití uživatelského jména a hesla mělo za důsledek nedostupnost několik měsíců**

Co se děje a jak je to vůbec možné?

Chtěl bych se s Vámi podělit o několik skutečných příběhů z forenzního vyšetřování.

- ✓ Uživatel klikne na nevhodný e-mail a zašifruje celou firmu
- ✓ Někdo otevře infikovaný soubor s malware a způsobí nedostupnost systémů
- ✓ Nepoužívání MFA na VPN s kombinací zneužití uživatelského jména a hesla mělo za důsledek nedostupnost několik měsíců
- ✓ Plochá síť propojená do fabrik na 4 kontinentech způsobila kolaps a šíření malware v řádu minut

Co se děje a jak je to vůbec možné?

Chtěl bych se s Vámi podělit o několik skutečných příběhů z forenzního vyšetřování.

- ✓ **Uživatel klikne na nevhodný e-mail a zašifruje celou firmu**
- ✓ **Někdo otevře infikovaný soubor s malware a způsobí nedostupnost systémů**
- ✓ **Nepoužívání MFA na VPN s kombinací zneužití uživatelského jména a hesla mělo za důsledek nedostupnost několik měsíců**
- ✓ **Plochá síť propojená do fabrik na 4 kontinentech způsobila kolaps a šíření malware v řádu minut**
- ✓ **Zranitelnost na perimetru v jednom systému zašifrovala celou firmu**

Co se děje a jak je to vůbec možné?

Chtěl bych se s Vámi podělit o několik skutečných příběhů z forenzního vyšetřování.

- ✓ **Uživatel klikne na nevhodný e-mail a zašifruje celou firmu**
- ✓ **Někdo otevře infikovaný soubor s malware a způsobí nedostupnost systémů**
- ✓ **Nepoužívání MFA na VPN s kombinací zneužití uživatelského jména a hesla mělo za důsledek nedostupnost několik měsíců**
- ✓ **Plochá síť propojená do fabrik na 4 kontinentech způsobila kolaps a šíření malware v řádu minut**
- ✓ **Zranitelnost na perimetru v jednom systému zašifrovala celou firmu**
- ✓ **Neaktualizovaná webová služba umožnila přístup komukoliv do interní firemní sítě**



Tipy z praxe

Tipy z praxe jak ...

... zabezpečit zálohy a nepřijít o ně

... zabezpečit data ,tak aby byli snadno obnovitelné a verzované

... ochránit perimetr firmy svépomocí



Zabezpečení záloh

Jak zabezpečit zálohy?

Správně nastavená zálohovací architektura znemožní útočníkovi získat přístup k zálohám a zničit je.

Checklist záloh:

- ✓ Pravidlo **3-2-1+1**

Jak zabezpečit zálohy?

Správně nastavená zálohovací architektura znemožní útočníkovi získat přístup k zálohám a zničit je.

Jak zabezpečit zálohy?

Správně nastavená zálohovací architektura znemožní útočníkovi získat přístup k zálohám a zničit je.

Checklist záloh:

- ✓ Pravidlo **3-2-1+1**
- ✓ Pravidelná **kontrola úplnosti a funkčnost záloh**

Jak zabezpečit zálohy?

Správně nastavená zálohovací architektura znemožní útočníkovi získat přístup k zálohám a zničit je.

Checklist záloh:

- ✓ Pravidlo **3-2-1+1**
- ✓ Pravidelná **kontrola úplnosti a funkčnosti záloh**
- ✓ **Oddělení záloh a virtualizace od Windows domény**

Jak zabezpečit zálohy?

Správně nastavená zálohovací architektura znemožní útočnickovi získat přístup k zálohám a zničit je.

Checklist záloh:

- ✓ Pravidlo **3-2-1+1**
- ✓ Pravidelná **kontrola úplnosti a funkčnosti záloh**
- ✓ **Oddělení záloh a virtualizace od Windows domény**
- ✓ **Vlastní VLAN pro zálohování s minimálními prostupy**

Jak zabezpečit zálohy?

Správně nastavená zálohovací architektura znemožní útočníkovi získat přístup k zálohám a zničit je.

Checklist záloh:

- ✓ Pravidlo **3-2-1+1**
- ✓ Pravidelná **kontrola úplnosti a funkčnosti záloh**
- ✓ **Oddělení záloh a virtualizace** od Windows domény
- ✓ **Vlastní VLAN pro zálohování** s minimálními prostupy
- ✓ Historie záloh

Jak zabezpečit zálohy?

Správně nastavená zálohovací architektura znemožní útočnickovi získat přístup k zálohám a zničit je.

Checklist záloh:

- ✓ Pravidlo **3-2-1+1**
- ✓ Pravidelná **kontrola úplnosti a funkčnosti záloh**
- ✓ **Oddělení záloh a virtualizace** od Windows domény
- ✓ **Vlastní VLAN pro zálohování** s minimálními prostupy
- ✓ Historie záloh
- ✓ Co cloud? Zálohujete? např. o365

Jak zabezpečit zálohy?

Správně nastavená zálohovací architektura znemožní útočnickovi získat přístup k zálohám a zničit je.

Checklist záloh:

- ✓ Pravidlo **3-2-1+1**
- ✓ Pravidelná **kontrola úplnosti a funkčnosti záloh**
- ✓ **Oddělení záloh a virtualizace** od Windows domény
- ✓ **Vlastní VLAN pro zálohování** s minimálními prostupy
- ✓ Historie záloh
- ✓ Co cloud? Zálohujete? např. o365
- ✓ **Disaster Recovery plán**

Jak zabezpečit zálohy?

Správně nastavená zálohovací architektura znemožní útočnickovi získat přístup k zálohám a zničit je.

Checklist záloh:

- ✓ Pravidlo 3-2-1+1
- ✓ Pravidelná kontrola úplnosti a funkčnost záloh
- ✓ Oddělení záloh a virtualizace od Windows domény
- ✓ Vlastní VLAN pro zálohování s minimálními prostupy
- ✓ Historie záloh
- ✓ Co cloud? Zálohujete? např. o365
- ✓ Disaster Recovery plán
- ✓ Časy RPO, RTO - BCP

Jak zabezpečit zálohy?

Správně nastavená zálohovací architektura znemožní útočníkovi získat přístup k zálohám a zničit je.

Checklist záloh:

- ✓ Pravidlo 3-2-1+1
- ✓ Pravidelná kontrola úplnosti a funkčnost záloh
- ✓ Oddělení záloh a virtualizace od Windows domény
- ✓ Vlastní VLAN pro zálohování s minimálními prostupy
- ✓ Historie záloh
- ✓ Co cloud? Zálohujete? např. o365
- ✓ Disaster Recovery plán
- ✓ Časy RPO, RTO - BCP
- ✓ Cloud backup

Jak zabezpečit zálohy?

Správně nastavená zálohovací architektura znemožní útočnickovi získat přístup k zálohám a zničit je.



Checklist záloh:

- ✓ Pravidlo 3-2-1+1
- ✓ Pravidelná kontrola úplnosti a funkčnosti záloh
- ✓ Oddělení záloh a virtualizace od Windows domény
- ✓ Vlastní VLAN pro zálohování s minimálními prostupy
- ✓ Historie záloh
- ✓ Co cloud? Zálohujete? např. o365
- ✓ Disaster Recovery plán
- ✓ Časy RPO, RTO - BCP
- ✓ Cloud backup

Jak zabezpečit zálohy?

Správně nastavená zálohovací architektura znemožní útočnickovi získat přístup k zálohám a zničit je.



Checklist záloh:

- ✓ Pravidlo 3-2-1+1
- ✓ Pravidelná kontrola úplnosti a funkčnosti záloh
- ✓ Oddělení záloh a virtualizace od Windows domény
- ✓ Vlastní VLAN pro zálohování s minimálními prostupy
- ✓ Historie záloh
- ✓ Co cloud? Zálohujete? např. o365
- ✓ Disaster Recovery plán
- ✓ Časy RPO, RTO - BCP
- ✓ Cloud backup

Jak zabezpečit zálohy?

Správně nastavená zálohovací architektura znemožní útočnickovi získat přístup k zálohám a zničit je.



Checklist záloh:

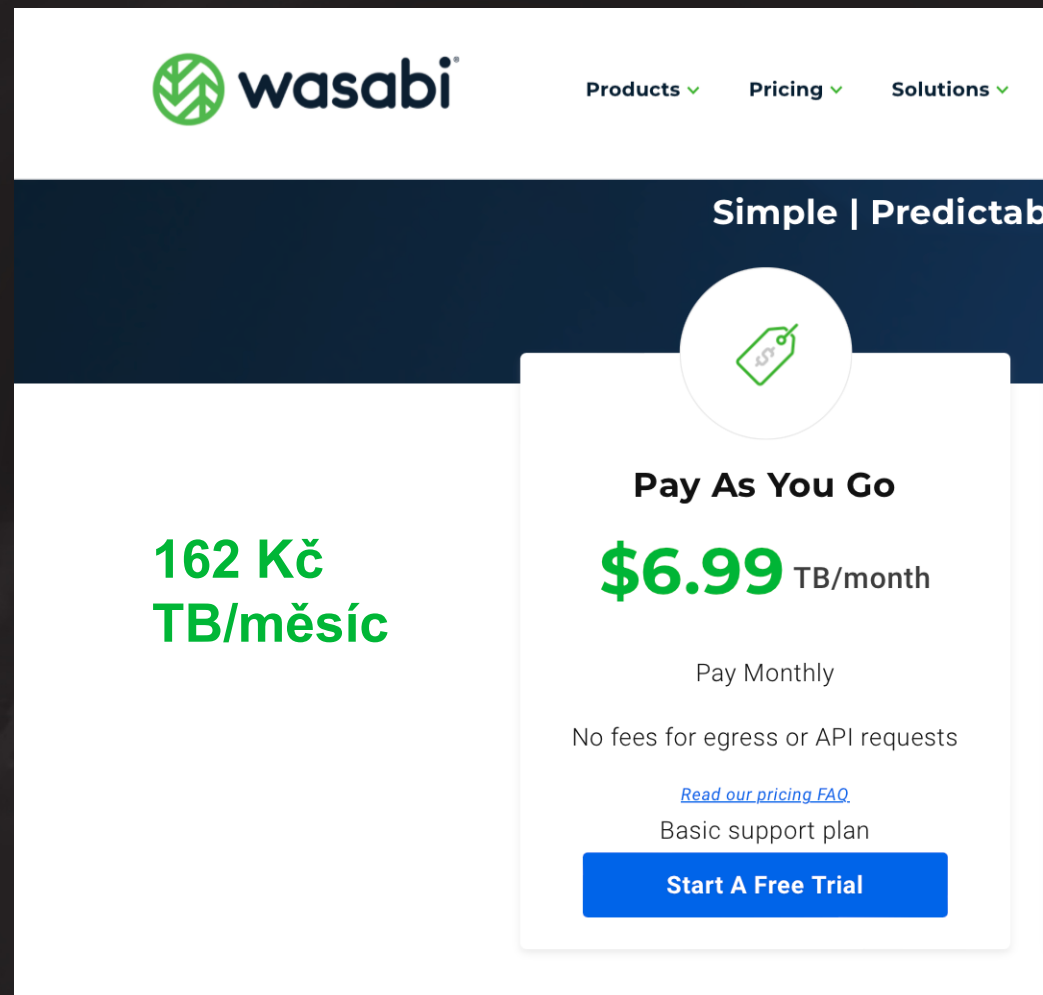
- ✓ Pravidlo 3-2-1+1
- ✓ Pravidelná kontrola úplnosti a funkčnosti záloh
- ✓ Oddělení záloh a virtualizace od Windows domény
- ✓ Vlastní VLAN pro zálohování s minimálními prostupy
- ✓ Historie záloh
- ✓ Co cloud? Zálohujete? např. o365
- ✓ Disaster Recovery plán
- ✓ Časy RPO, RTO - BCP
- ✓ Cloud backup

Jak zabezpečit zálohy?

Správně nastavená zálohovací architektura znemožní útočnickovi získat přístup k zálohám a zničit je.



Checklist záloh:



wasabi

Products ▾ Pricing ▾ Solutions ▾

Simple | Predictable

Pay As You Go

\$6.99 TB/month

Pay Monthly

No fees for egress or API requests

[Read our pricing FAQ](#)

Basic support plan

[Start A Free Trial](#)

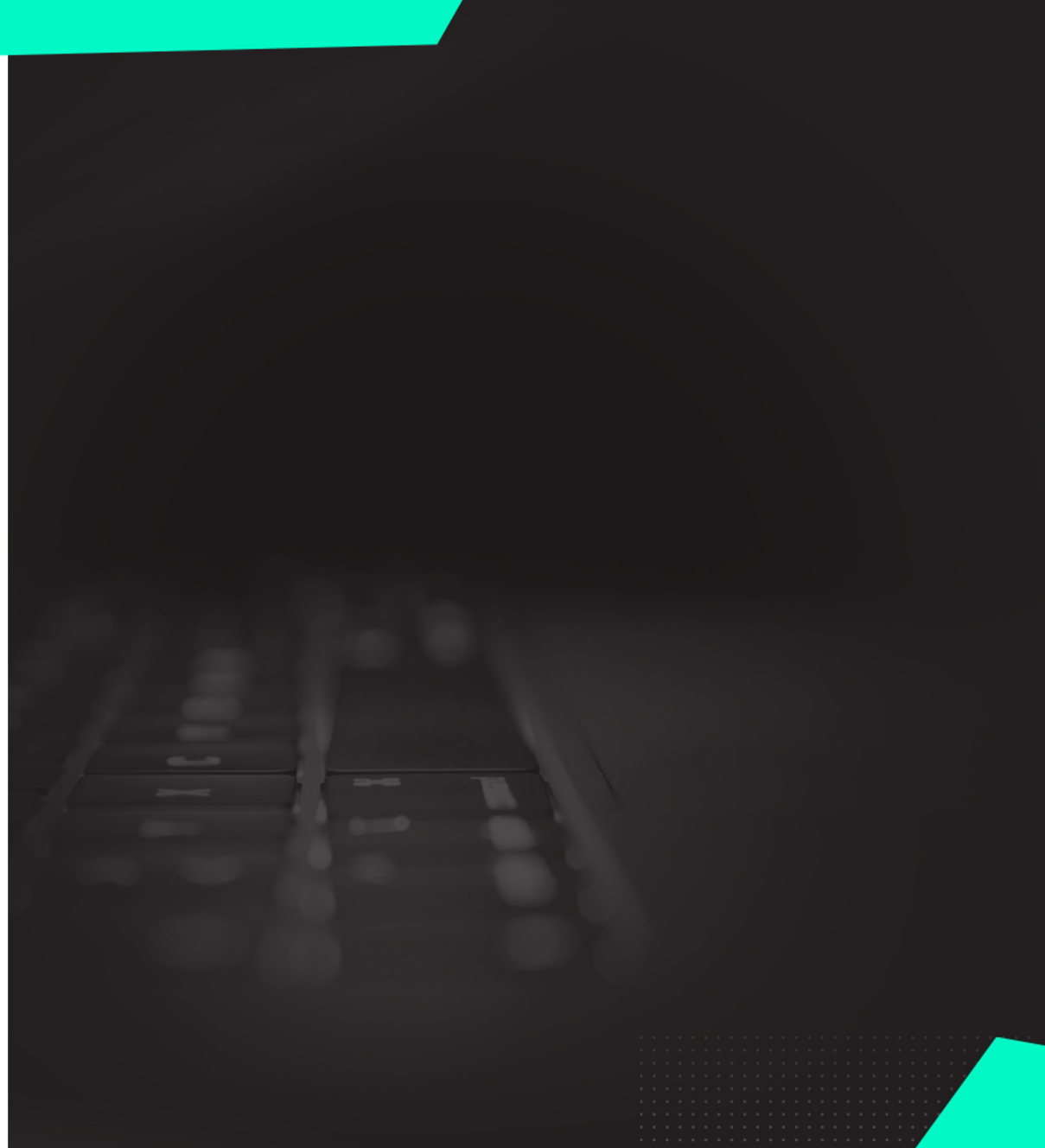
<https://wasabi.com/cloud-storage-pricing/#three-info>



Jak ukládat data a zálohy kyberbezpečně

Jak ukládat data a zálohy?

Velmi často vidíme data a zálohy na NAS zařízeních např. Synology, QNAP, TrueNAS, ale tyto zařízení jsou **VŽDY** nedostatečně zabezpečeny z pohledu kybernetické bezpečnosti.



Jak ukládat data a zálohy?

Velmi často vidíme data a zálohy na NAS zařízeních např. Synology, QNAP, TrueNAS, ale tyto zařízení jsou **VŽDY** nedostatečně zabezpečeny z pohledu kybernetické bezpečnosti.

Checklist NAS:

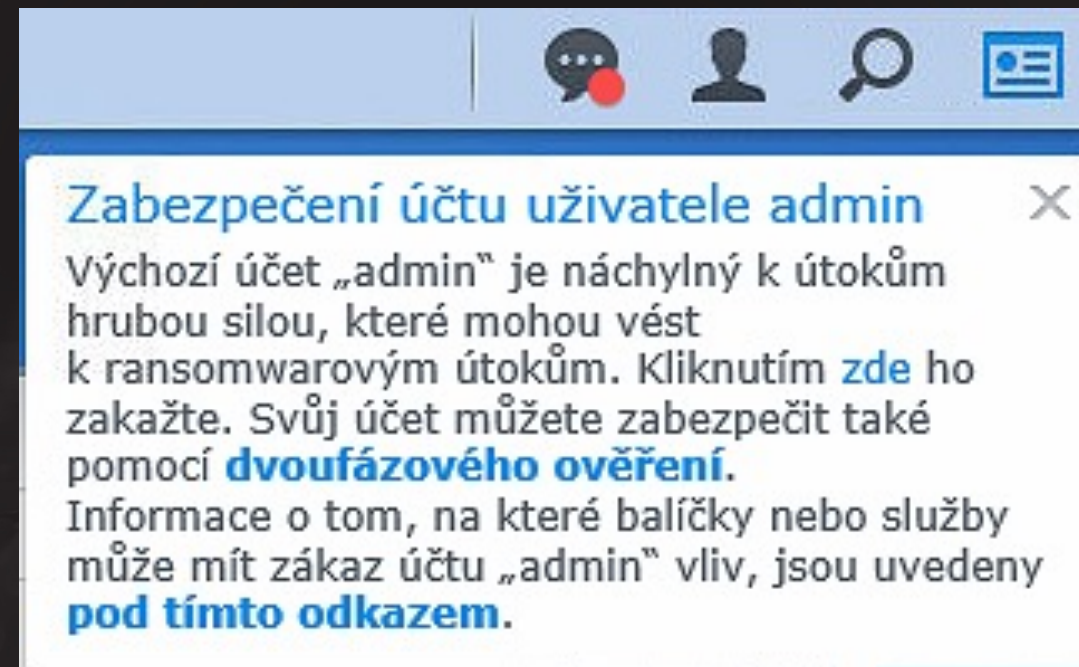
- ✓ Silné metody ověřování pro ADMIN účty

Jak ukládat data a zálohy?

Velmi často vidíme data a zálohy na NAS zařízeních např. Synology, QNAP, TrueNAS, ale tyto zařízení jsou **VŽDY** nedostatečně zabezpečeny z pohledu kybernetické bezpečnosti.

Checklist NAS:

- ✓ Silné metody ověřování pro ADMIN účty



Jak ukládat data a zálohy?

Velmi často vidíme data a zálohy na NAS zařízeních např. Synology, QNAP, TrueNAS, ale tyto zařízení jsou **VŽDY** nedostatečně zabezpečeny z pohledu kybernetické bezpečnosti.

Checklist NAS:

- ✓ Silné metody ověřování pro ADMIN účty
 - ✓ Integrované, silné, jednoduché, **ZDARMA**

Jak ukládat data a zálohy?

Velmi často vidíme data a zálohy na NAS zařízeních např. Synology, QNAP, TrueNAS, ale tyto zařízení jsou **VŽDY** nedostatečně zabezpečeny z pohledu kybernetické bezpečnosti.

Checklist NAS:

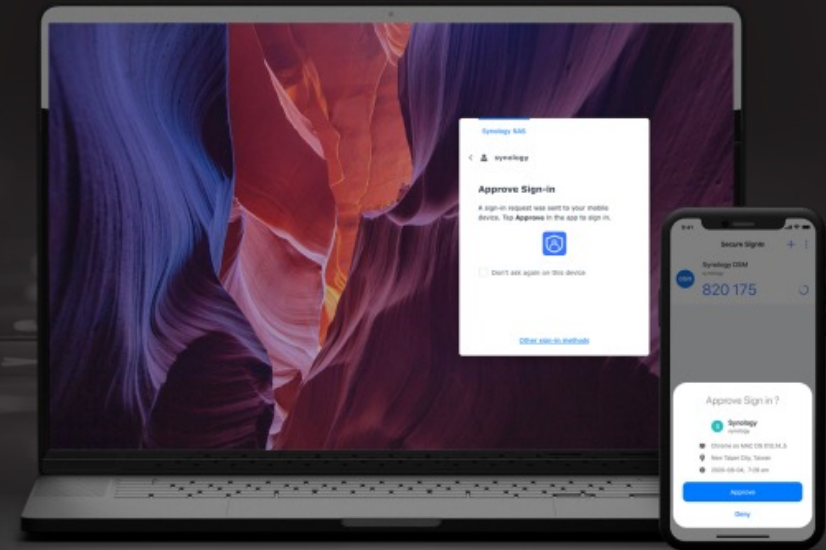
- ✓ Silné metody ověřování pro ADMIN účty
 - ✓ Integrované, silné, jednoduché, **ZDARMA**
 - ✓ MFA
 - ✓ FIDO
 - ✓ Passwordless

Jak ukládat data a zálohy?

Velmi často vidíme data a zálohy na NAS zařízeních např. Synology, QNAP, TrueNAS, ale tyto zařízení jsou **VŽDY** nedostatečně zabezpečeny z pohledu kybernetické bezpečnosti.

Checklist NAS:

- ✓ Silné metody ověřování pro ADMIN účty
 - ✓ Integrované, silné, jednoduché, **ZDARMA**
 - ✓ MFA
 - ✓ FIDO
 - ✓ Passwordless



<https://www.synology.com/cs-cz/dsm/feature/authentication>

<https://www.qnap.com/solution/authentication/en-us/>

<https://www.truenas.com/docs/core/uireference/system/2fa/>

Jak ukládat data a zálohy?

Velmi často vidíme data a zálohy na NAS zařízeních např. Synology, QNAP, TrueNAS, ale tyto zařízení jsou **VŽDY** nedostatečně zabezpečeny z pohledu kybernetické bezpečnosti.

Checklist NAS:

- ✓ **Historie záloh**
 - ✓ Zálohovací software řeší retenci záloh
 - ✓ Snapshoty a Replikace - ochrana dat na úrovni bloků HDD
 - ✓ **MUSÍ se ručně instalovat !**
 - ✓ Podmínka BTRFS



Snapshot Replication

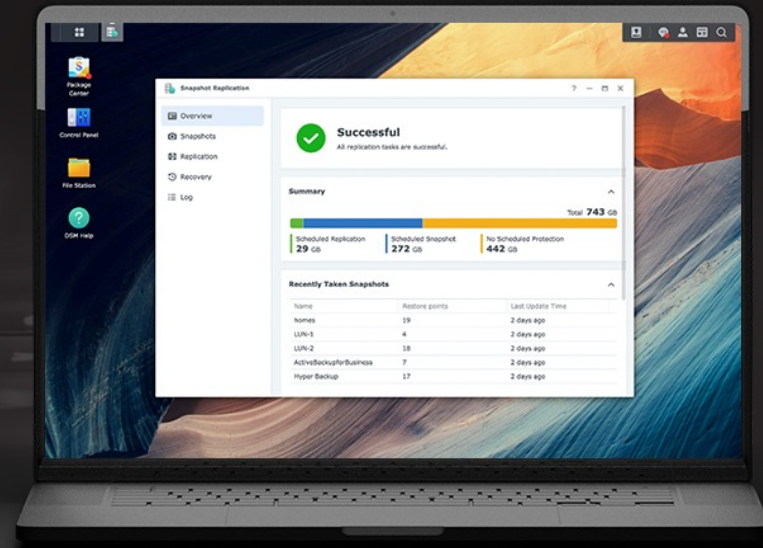
<https://www.synology.com/en-global/dsm/packages/SnapshotReplication>

Jak ukládat data a zálohy?

Velmi často vidíme data a zálohy na NAS zařízeních např. Synology, QNAP, TrueNAS, ale tyto zařízení jsou **VŽDY** nedostatečně zabezpečeny z pohledu kybernetické bezpečnosti.

Checklist NAS:

- ✓ Historie záloh
 - ✓ Zálohovací software řeší retenci záloh
 - ✓ Snapshoty a Replikace - ochrana dat na úrovni bloků HDD
 - ✓ **MUSÍ se ručně instalovat !**
 - ✓ **Podmínka BTRFS**
 - ✓ Lokální replikace



https://www.synology.com/en-global/dsm/feature/snapshot_replication

<https://www.qnap.com/solution/home-snapshots/en/>

<https://www.truenas.com/docs/core/coretutorials/storage/snapshots/>

Jak ukládat data a zálohy?

Velmi často vidíme data a zálohy na NAS zařízeních např. Synology, QNAP, TrueNAS, ale tyto zařízení jsou **VŽDY** nedostatečně zabezpečeny z pohledu kybernetické bezpečnosti.

Checklist NAS:

- ✓ Historie záloh
 - ✓ Zálohovací software řeší retenci záloh
 - ✓ Snapshoty a Replikace - ochrana dat na úrovni bloků HDD
 - ✓ **MUSÍ se ručně instalovat !**
 - ✓ Podmínka BTRFS
 - ✓ Lokální replikace
 - ✓ Vzdálená replikace



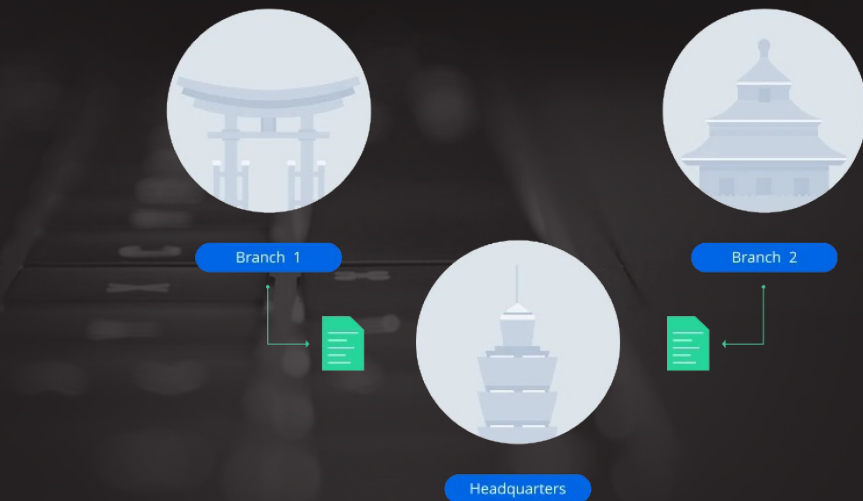
https://www.synology.com/en-global/dsm/feature/snapshot_replication
<https://www.qnap.com/solution/home-snapshots/en/>
<https://www.truenas.com/docs/core/coretutorials/storage/snapshots/>

Jak ukládat data a zálohy?

Velmi často vidíme data a zálohy na NAS zařízeních např. Synology, QNAP, TrueNAS, ale tyto zařízení jsou **VŽDY** nedostatečně zabezpečeny z pohledu kybernetické bezpečnosti.

Checklist NAS:

- ✓ **Historie záloh**
 - ✓ Zálohovací software řeší retenci záloh
 - ✓ Snapshoty a Replikace - ochrana dat na úrovni bloků HDD
 - ✓ **MUSÍ se ručně instalovat !**
 - ✓ Podmínka BTRFS
 - ✓ Lokální replikace
 - ✓ Vzdálená replikace
 - ✓ Replikace poboček na centrálu



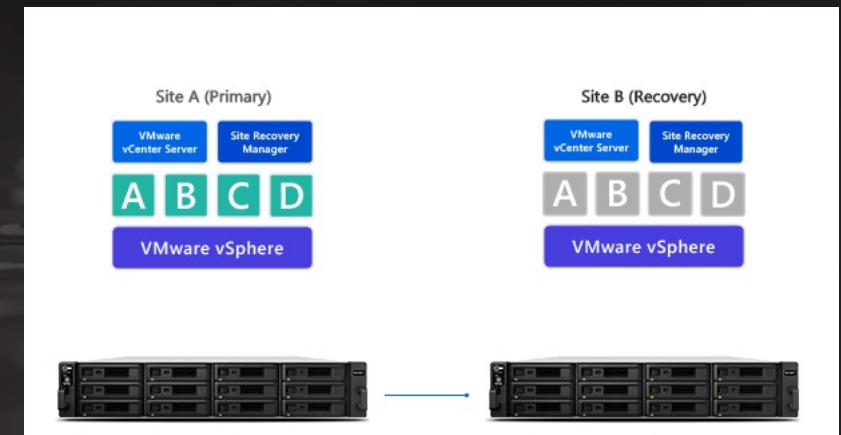
https://www.synology.com/en-global/dsm/feature/snapshot_replication
<https://www.qnap.com/solution/home-snapshots/en/>
<https://www.truenas.com/docs/core/coretutorials/storage/snapshots/>

Jak ukládat data a zálohy?

Velmi často vidíme data a zálohy na NAS zařízeních např. Synology, QNAP, TrueNAS, ale tyto zařízení jsou **VŽDY** nedostatečně zabezpečeny z pohledu kybernetické bezpečnosti.

Checklist NAS:

- ✓ **Historie záloh**
 - ✓ Zálohovací software řeší retenci záloh
 - ✓ Snapshoty a Replikace - ochrana dat na úrovni bloků HDD
 - ✓ **MUSÍ se ručně instalovat !**
 - ✓ Podmínka BTRFS
 - ✓ Lokální replikace
 - ✓ Vzdálená replikace
 - ✓ Replikace poboček na centrálu
 - ✓ Replikace pro virtualizační platformy



https://www.synology.com/en-global/dsm/feature/snapshot_replication

<https://www.qnap.com/solution/home-snapshots/en/>

<https://www.truenas.com/docs/core/coretutorials/storage/snapshots/>



Ochrana perimetru

Checklist PERIMETR:

- ✓ Exponované služby

Jak chráníte perimetr firmy?

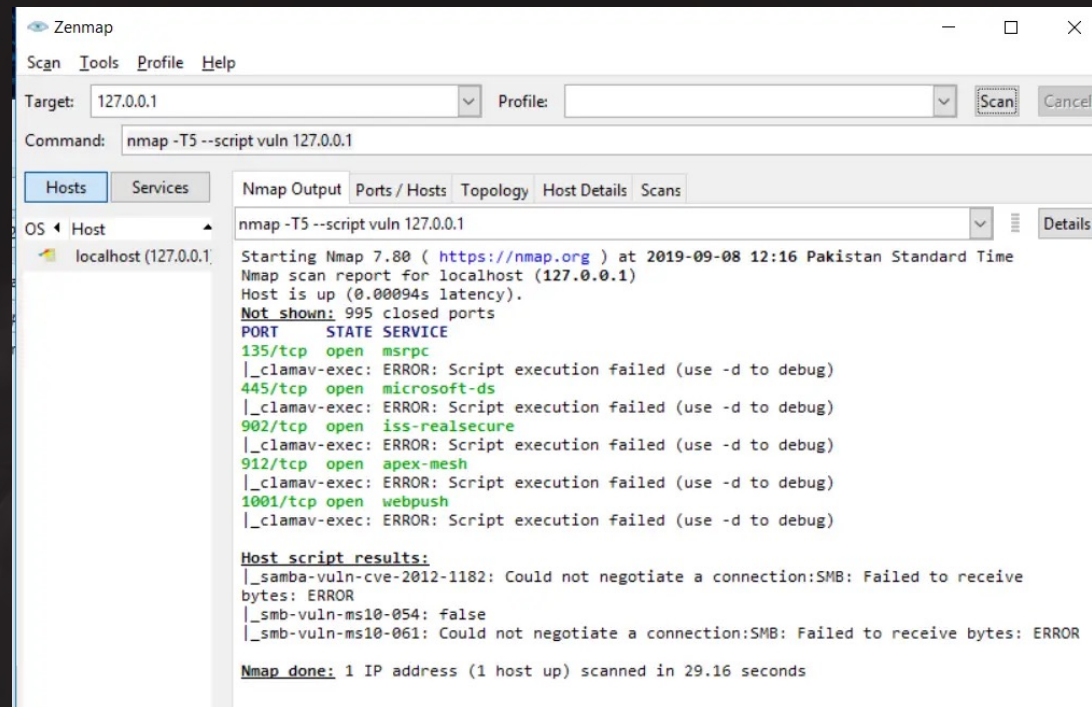
Firewall,,, jasný Víte, ale jaké máte exponované služby do sítě internet? Vlastně zároveň do celého světa? Jaké chyby, zranitelnosti tam jsou, o kterých možná ani nevíte?

Jak chráníte perimetr firmy?

Firewall,,, jasný Víte, ale jaké máte exponované služby do sítě internet? Vlastně zároveň do celého světa? Jaké chyby, zranitelnosti tam jsou, o kterých možná ani nevíte?

Checklist PERIMETR:

✓ Exponované služby



```
zenmap
Scan Tools Profile Help
Target: 127.0.0.1 Profile: Scan Cancel
Command: nmap -T5 --script vuln 127.0.0.1
Hosts Services Nmap Output Ports/Hosts Topology Host Details Scans
OS Host localhost (127.0.0.1)
nmap -T5 --script vuln 127.0.0.1
Starting Nmap 7.80 ( https://nmap.org ) at 2019-09-08 12:16 Pakistan Standard Time
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00094s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
445/tcp   open  microsoft-ds
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
902/tcp   open  iss-realsecure
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
912/tcp   open  apex-mesh
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
1001/tcp  open  webpush
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
Host script results:
|_samba-vuln-cve-2012-1182: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR
Nmap done: 1 IP address (1 host up) scanned in 29.16 seconds
```

<https://nmap.org>

Jak chráníte perimetr firmy?

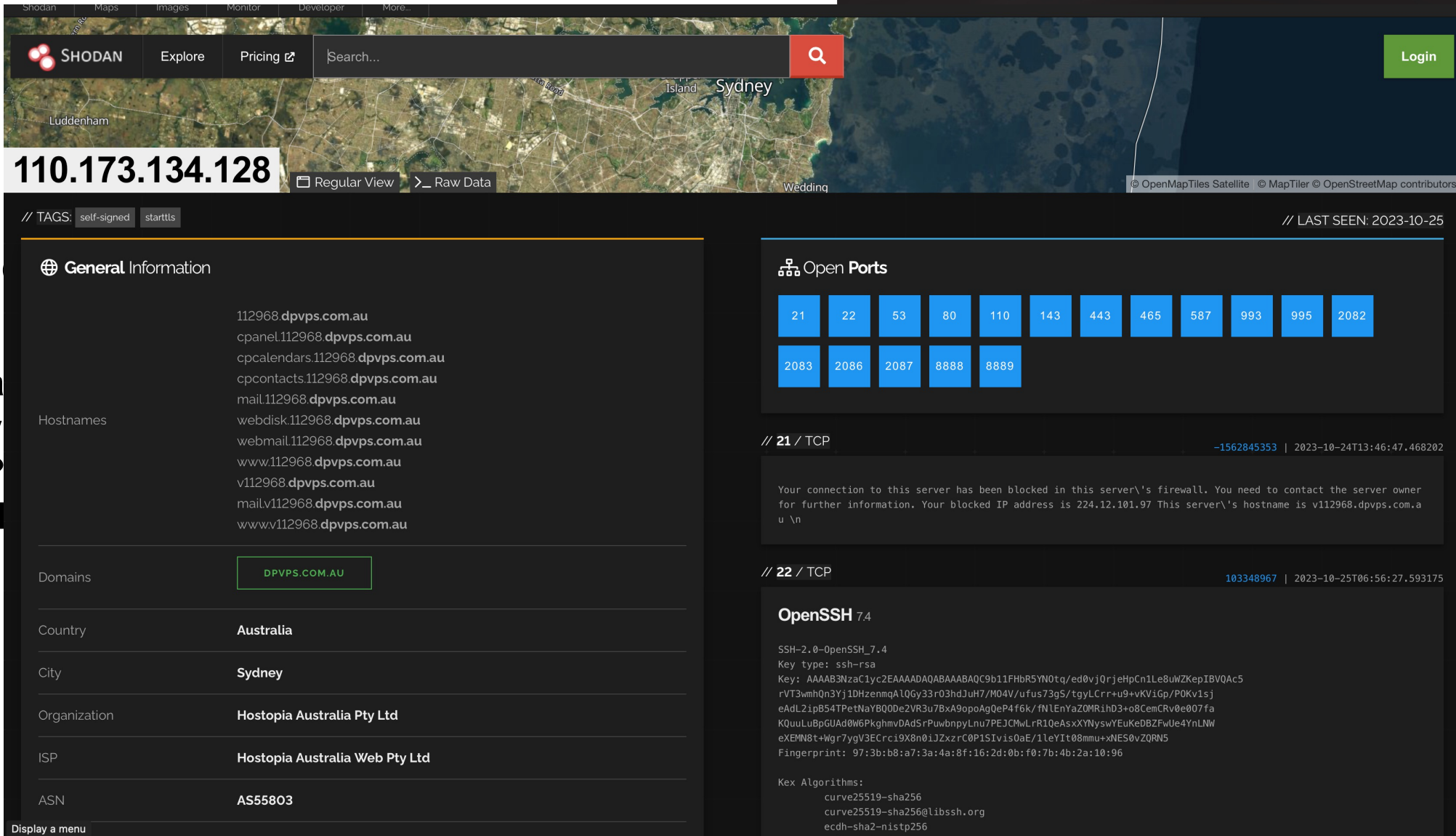
Firewall,,, jasný Víte, ale jaké máte exponované služby do sítě internet? Vlastně zároveň do celého světa? Jaké chyby, zranitelnosti tam jsou, o kterých možná ani nevíte?

Checklist PERIMETR:

- ✓ Exponované služby
- ✓ Fingerprint služeb a jejich verze

<https://nmap.org>

Jak
Firewa
služby
světa?
kterýc



SHODAN Explore Pricing Search... Login

110.173.134.128 Regular View Raw Data

// TAGS: self-signed starttls // LAST SEEN: 2023-10-25

General Information

112968.dpvps.com.au
cpanel.112968.dpvps.com.au
cpcalendars.112968.dpvps.com.au
cpcontacts.112968.dpvps.com.au
mail.112968.dpvps.com.au
Hostnames
webdisk.112968.dpvps.com.au
webmail.112968.dpvps.com.au
www.112968.dpvps.com.au
v112968.dpvps.com.au
mailv112968.dpvps.com.au
wwwv112968.dpvps.com.au

Domains **DPVPS.COM.AU**

Country **Australia**

City **Sydney**

Organization **Hostopia Australia Pty Ltd**

ISP **Hostopia Australia Web Pty Ltd**

ASN **AS55803**

Open Ports

21	22	53	80	110	143	443	465	587	993	995	2082
2083	2086	2087	8888	8889							

// 21 / TCP -1562845353 | 2023-10-24T13:46:47.468202

Your connection to this server has been blocked in this server's firewall. You need to contact the server owner for further information. Your blocked IP address is 224.12.101.97 This server's hostname is v112968.dpvps.com.au \n

// 22 / TCP 103348967 | 2023-10-25T06:56:27.593175

OpenSSH 7.4

SSH-2.0-OpenSSH_7.4
Key type: ssh-rsa
Key: AAAAB3NzaC1yc2EAAAADAQABAAQCA9b1FHbR5YN0tq/ed0vj0rjeHpCn1Le8uWZKepIBVQAc5rVT3wmhQn3Yj1DHzenmqALQgy33r03hdJUH7/M04V/uFus73gS/tygLcrr+u9+vKViGp/P0Kv1sjeAdL2ipB54TPetNaYBQ0De2VR3u7BxA9opoAgQeP4f6k/fn1EnYaZOMRihD3+o8CemCRV0e007faKQuuLuBpGUAd0W6PkgmVDAdSrPuwbnpyLnu7PEJCMwLrR1QeAsxYNYswYEuKeDBZFWUe4YnLNW eXEMN8t+Wgr7ygV3ECrc19X8n01JZxzrC0P1Sivis0aE/1leYIt08mmu+XNES0vZQRNS
Fingerprint: 97:3b:b8:a7:3a:4a:8f:16:2d:0b:f0:7b:4b:2a:10:96

Kex Algorithms:
curve25519-sha256
curve25519-sha256@libssh.org
ecdh-sha2-nistp256

Jak chráníte perimetr firmy?

Firewall,,, jasný Víte, ale jaké máte exponované služby do sítě internet? Vlastně zároveň do celého světa? Jaké chyby, zranitelnosti tam jsou, o kterých možná ani nevíte?

Checklist PERIMETR:

- ✓ Exponované služby
- ✓ Fingerprint služeb a jejich verze
- ✓ Zranitelnosti

<https://nmap.org>
<https://www.shodan.io>

Jak chráníte perimet

Firewall,,, jasný Víte, a
služby do sítě internet?
světa? Jaké chyby, z
kterých možná ani nevíte

ISP Hostopia Australia Web Pty Ltd

ASN AS55803

Vulnerabilities

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

CVE-2023-38408 The PKCS#11 feature in ssh-agent in OpenSSH before 9.3p2 has an insufficiently trustworthy search path, leading to remote code execution if an agent is forwarded to an attacker-controlled system. (Code in /usr/lib is not necessarily safe for loading into ssh-agent.) NOTE: this issue exists because of an incomplete fix for CVE-2016-10009.

CVE-2021-41617 **4.4** sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

CVE-2021-36368 **2.6** **** DISPUTED **** An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is "this is not an authentication bypass, since nothing is being bypassed."

CVE-2020-15778 **6.8** **** DISPUTED **** scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of "anomalous argument transfers" because that could "stand a great chance of breaking existing workflows."

CVE-2020-10541 **4.3** The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy

PERIMETR:

né služby

it služeb a jejich verze

sti



Kolik to stojí?

Kolik to stojí?

Ceník:

- ✓ Kolik stojí aktualizace OS serverů a stanic?

Kolik to stojí?

Ceník:

- ✓ Kolik stojí aktualizace OS serverů a stanic?
- ✓ Kolik stojí pravidelně kontrolovat záloh?

Kolik to stojí?

Ceník:

- ✓ Kolik stojí aktualizace OS serverů a stanic?
- ✓ Kolik stojí pravidelně kontrolovat záloh?
- ✓ Kolik stojí segmentace sítě?

Kolik to stojí?

Ceník:

- ✓ Kolik stojí aktualizace OS serverů a stanic?
- ✓ Kolik stojí pravidelně kontrolovat záloh?
- ✓ Kolik stojí segmentace sítě?
- ✓ Kolik stojí pravidelná kontrola perimetru?

Kolik to stojí?

Ceník:

- ✓ Kolik stojí aktualizace OS serverů a stanic?
- ✓ Kolik stojí pravidelně kontrolovat záloh?
- ✓ Kolik stojí segmentace sítě?
- ✓ Kolik stojí pravidelná kontrola perimetru?
- ✓ Kolik stojí používání MFA a unikátních hesel?

Kolik to stojí?

Ceník:

- ✓ Kolik stojí aktualizace OS serverů a stanic?
- ✓ Kolik stojí pravidelně kontrolovat záloh?
- ✓ Kolik stojí segmentace sítě?
- ✓ Kolik stojí pravidelná kontrola perimetru?
- ✓ Kolik stojí používání MFA a unikátních hesel?
- ✓ Kolik stojí sebevzdělávání?

Kolik to stojí?

Zde vidíte, že to není JEN o technologiích ale HLAVNĚ o konfiguraci a tvrdé práci IT správce. Viděl jsem nespočet kybernetických útoků. **Bohužel ne všechny útoky míří na uživatele, ale všechny útoky potřebovali privilegované oprávnění IT správce systému.**

Ceník:

- ✓ Kolik stojí aktualizace OS serverů a stanic?
- ✓ Kolik stojí pravidelně kontrolovat záloh?
- ✓ Kolik stojí segmentace sítě?
- ✓ Kolik stojí pravidelná kontrola perimetru?
- ✓ Kolik stojí používání MFA a unikátních hesel?
- ✓ Kolik stojí sebevzdělávání?



Alinet

Cyber Security, **Ransomware Incident Response**



Jakub Alimov

www.alinet.cz jakub.alimov@alinet.cz +420 774 077 108