Alinet

Zabezpečení dat i s nízkým rozpočtem

26.10.2023

Alinet CZ s.r.o. **mobil:** +420 774 077 108 **e-mail:** info@alinet.cz **web:** www.alinet.cz

Alinet

Kdo jsem?

Alinet

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/

Alinet CZ s.r.o. Pod Hájkem 406/1a, Praha 8, 180 00, CZ **mobil:** +420 774 077 108 **e-mail:** info@alinet.cz **web:** www.alinet.cz

Alinet

Kdo je Alinet?

Alinet

Jsme progresivní IT firma se specializací na kybernetické útoky.

DIGITAL FORENSICS AND INCIDENT RESPONSE

SLUŽBY KYBERNETICKÉ BEZPEČNOSTI

SLUŽBY DETEKCE KYBERNETICKÝCH UDÁLOSTÍ

Alinet CZ s.r.o. Pod Hájkem 406/1a, Praha 8, 180 00, CZ

mobil: +420 774 077 108 **e-mail:** info@alinet.cz **web:** www.alinet.cz

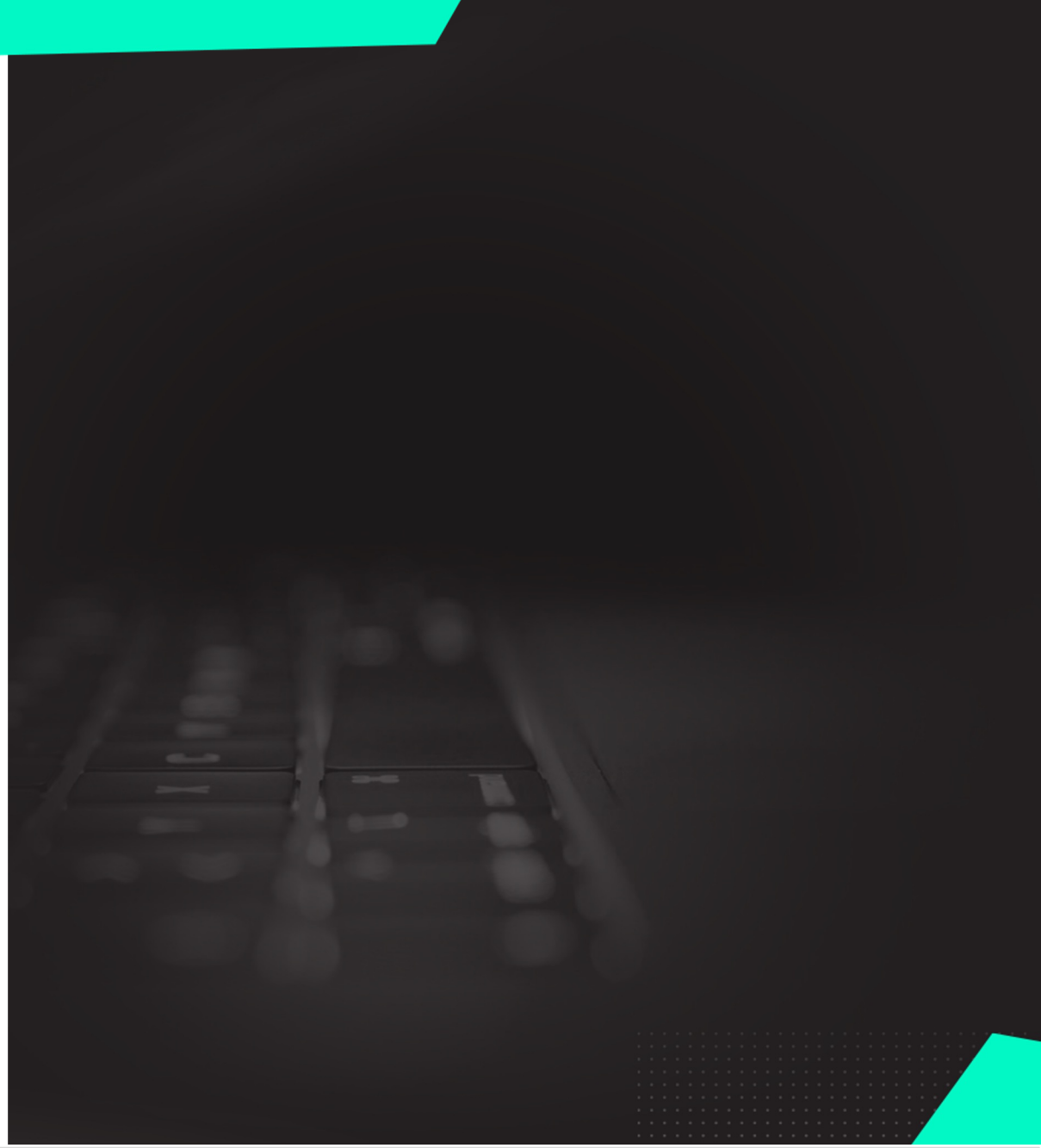
Alinet

Co se děje a jak je to vůbec možné?

Alinet

Co se děje a jak je to vůbec možné?

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



Alinet

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

Alinet

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**

Alinet

Co se děje a jak je to vůbec možné?

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

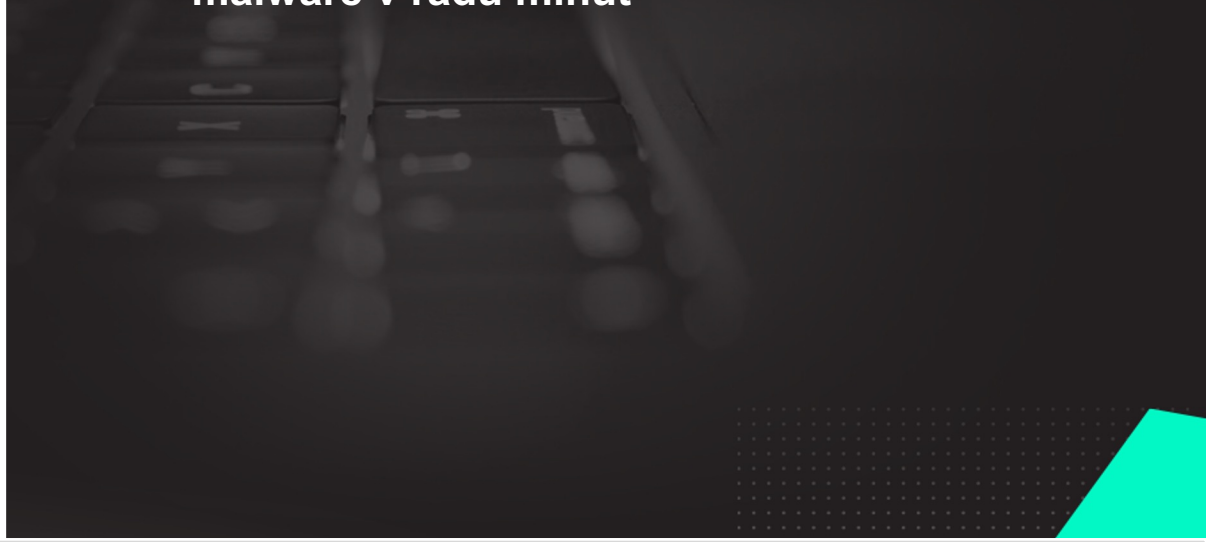
- ✓ Uživatel klikne na nevhodný e-mail a zašifruje celou firmu
- ✓ Někdo otevře infikovaný soubor s malware a způsobí nedostupnost systémů
- ✓ Nepoužívání MFA na VPN s kombinací zneužití uživatelského jména a hesla mělo za důsledek nedostupnost několik měsíců

Alinet

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



Alinet CZ s.r.o. Pod Hájkem 406/1a, Praha 8, 180 00, CZ

mobil: +420 774 077 108 **e-mail:** info@alinet.cz **web:** www.alinet.cz

Alinet

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

Alinet

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

Alinet

Tipy z praxe

Alinet

I. část:
Zabezpečení záloh

II. část:
Zabezpečení dat

III. část:
Ochrana perimteru

Tipy z praxe jak ...

… zabezpečit zálohy a nepřijít o ně

… zabezpečit data ,tak aby byli snadno obnovitelné a verzované

… ochránit perimetr firmy svépomocí

Alinet

Zabezpečení záloh

Alinet

Checklist záloh:

Jak zabezpečit zálohy?

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

Alinet

Jak zabezpečit zálohy?

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

Checklist záloh:

- ✓ **Pravidlo 3-2-1+1**

Alinet CZ s.r.o. Pod Hájkem 406/1a, Praha 8, 180 00, CZ

mobil: +420 774 077 108 **e-mail:** info@alinet.cz **web:** www.alinet.cz

Alinet

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

Alinet

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**

Alinet CZ s.r.o. Pod Hájkem 406/1a, Praha 8, 180 00, CZ

mobil: +420 774 077 108 **e-mail:** info@alinet.cz **web:** www.alinet.cz

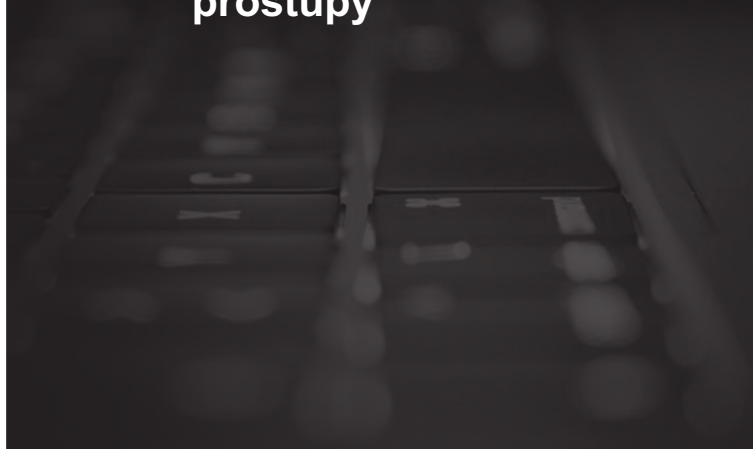
Alinet

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



Alinet CZ s.r.o. Pod Hájkem 406/1a, Praha 8, 180 00, CZ

mobil: +420 774 077 108 **e-mail:** info@alinet.cz **web:** www.alinet.cz

Alinet

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

Alinet CZ s.r.o. Pod Hájkem 406/1a, Praha 8, 180 00, CZ **mobil:** +420 774 077 108 **e-mail:** info@alinet.cz **web:** www.alinet.cz

Alinet

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

Alinet

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

Alinet CZ s.r.o. Pod Hájkem 406/1a, Praha 8, 180 00, CZ **mobil:** +420 774 077 108 **e-mail:** info@alinet.cz **web:** www.alinet.cz

Alinet

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

Alinet

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

Alinet CZ s.r.o. Pod Hájkem 406/1a, Praha 8, 180 00, CZ **mobil:** +420 774 077 108 **e-mail:** info@alinet.cz **web:** www.alinet.cz

Alinet

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

Alinet CZ s.r.o. Pod Hájkem 406/1a, Praha 8, 180 00, CZ **mobil:** +420 774 077 108 **e-mail:** info@alinet.cz **web:** www.alinet.cz

Alinet

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

Alinet CZ s.r.o. Pod Hájkem 406/1a, Praha 8, 180 00, CZ **mobil:** +420 774 077 108 **e-mail:** info@alinet.cz **web:** www.alinet.cz

Alinet

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

Alinet CZ s.r.o. Pod Hájkem 406/1a, Praha 8, 180 00, CZ **mobil:** +420 774 077 108 **e-mail:** info@alinet.cz **web:** www.alinet.cz

Alinet

Jak zabezpečit zálohy?

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

Checklist záloh:

wasabi

Products Pricing Solutions

Simple | Predictab

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

162 Kč TB/měsíc

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

Alinet CZ s.r.o. Pod Hájkem 406/1a, Praha 8, 180 00, CZ **mobil:** +420 774 077 108 **e-mail:** info@alinet.cz **web:** www.alinet.cz

Alinet

Jak ukládat data a zálohy kyberbezpečně

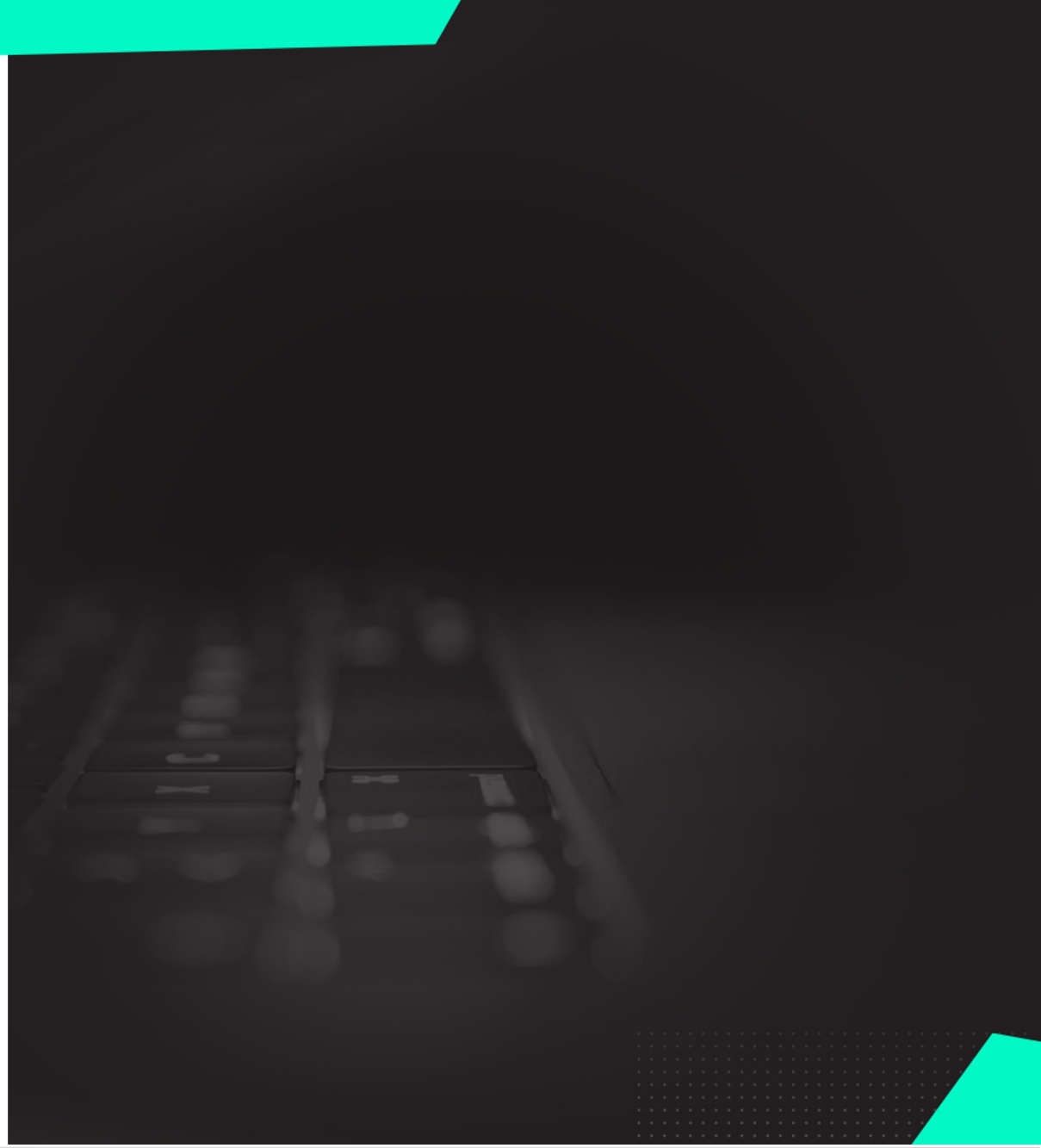
Alinet CZ s.r.o. Pod Hájkem 406/1a, Praha 8, 180 00, CZ

mobil: +420 774 077 108 **e-mail:** info@alinet.cz **web:** www.alinet.cz

Alinet

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.



Alinet

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**

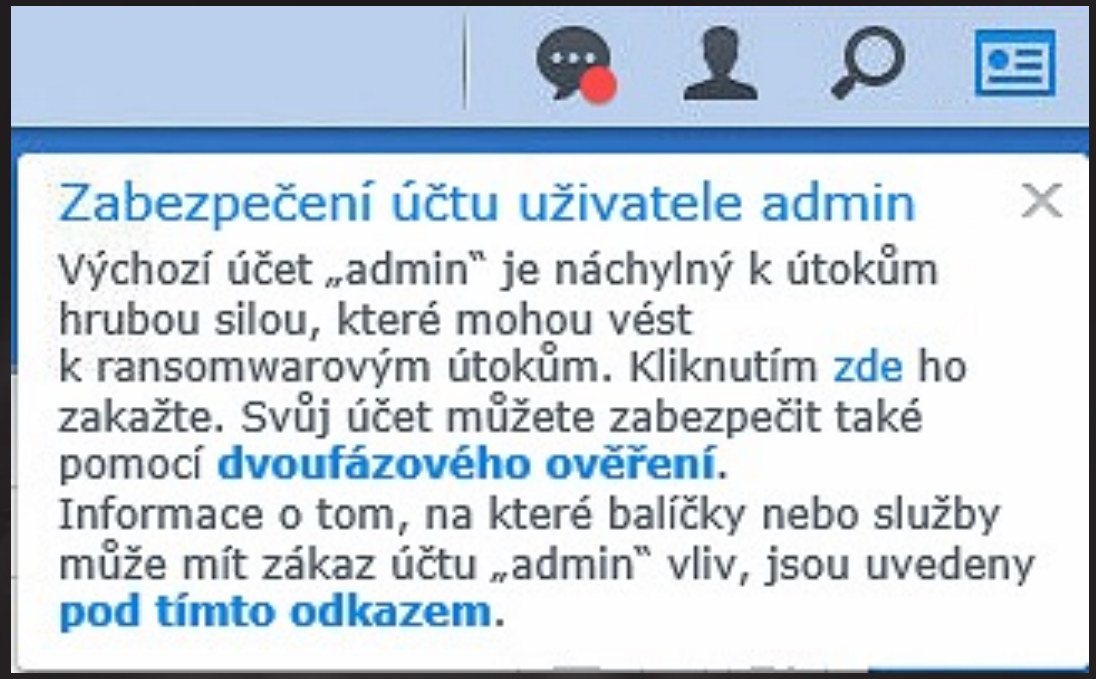
Alinet

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**



Alinet

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.

Alinet

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

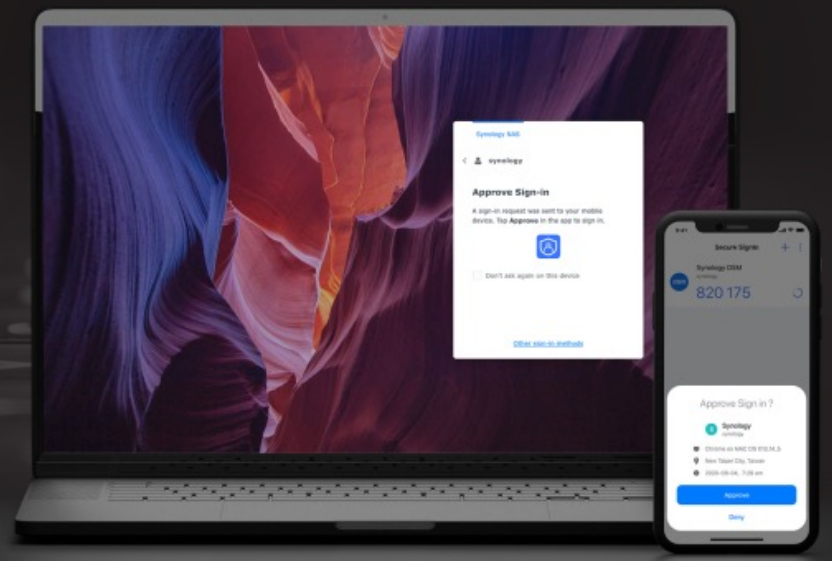
Alinet

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/

Alinet CZ s.r.o. Pod Hájkem 406/1a, Praha 8, 180 00, CZ **mobil:** +420 774 077 108 **e-mail:** info@alinet.cz **web:** www.alinet.cz

Alinet

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

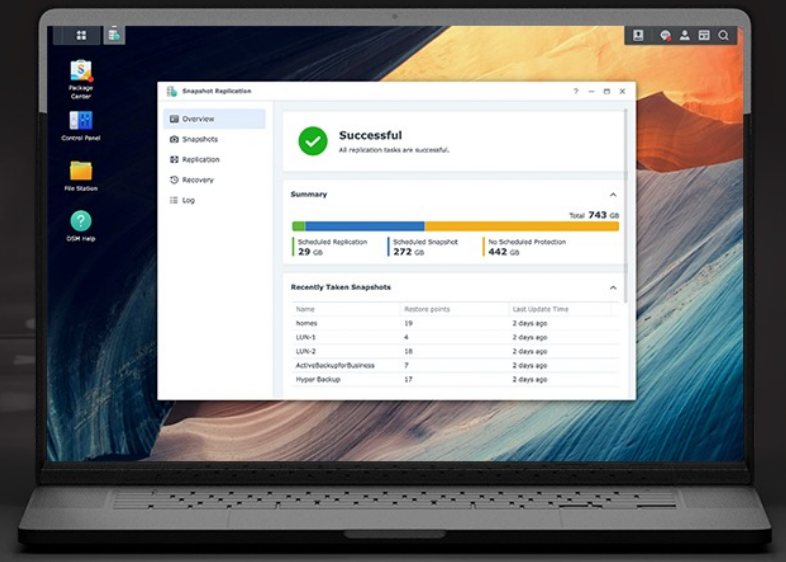
Alinet

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/

Alinet CZ s.r.o. Pod Hájkem 406/1a, Praha 8, 180 00, CZ **mobil:** +420 774 077 108 **e-mail:** info@alinet.cz **web:** www.alinet.cz

Alinet

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/

Alinet CZ s.r.o. Pod Hájkem 406/1a, Praha 8, 180 00, CZ **mobil:** +420 774 077 108 **e-mail:** info@alinet.cz **web:** www.alinet.cz

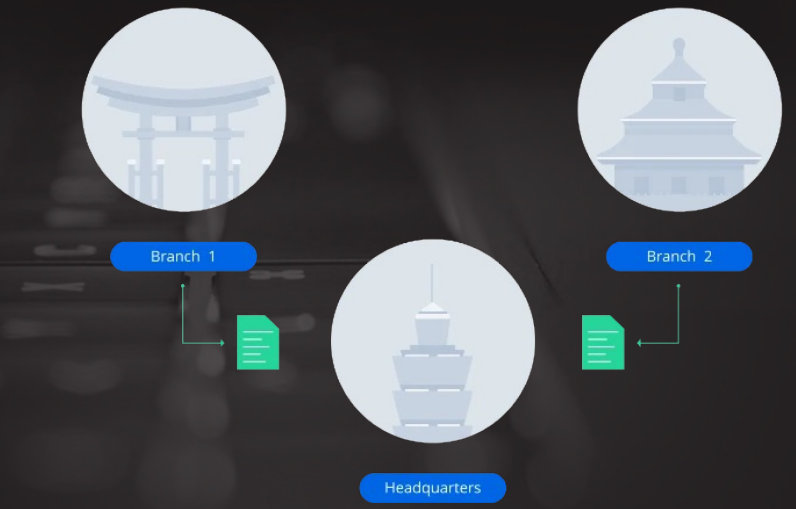
Alinet

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/

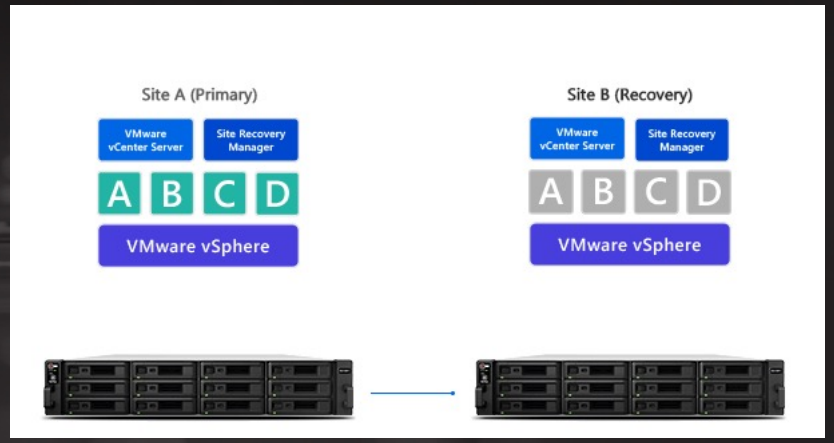
Alinet

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/

Alinet

Ochrana perimetru

Alinet CZ s.r.o. Pod Hájkem 406/1a, Praha 8, 180 00, CZ

mobil: +420 774 077 108 **e-mail:** info@alinet.cz **web:** www.alinet.cz

Alinet

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?

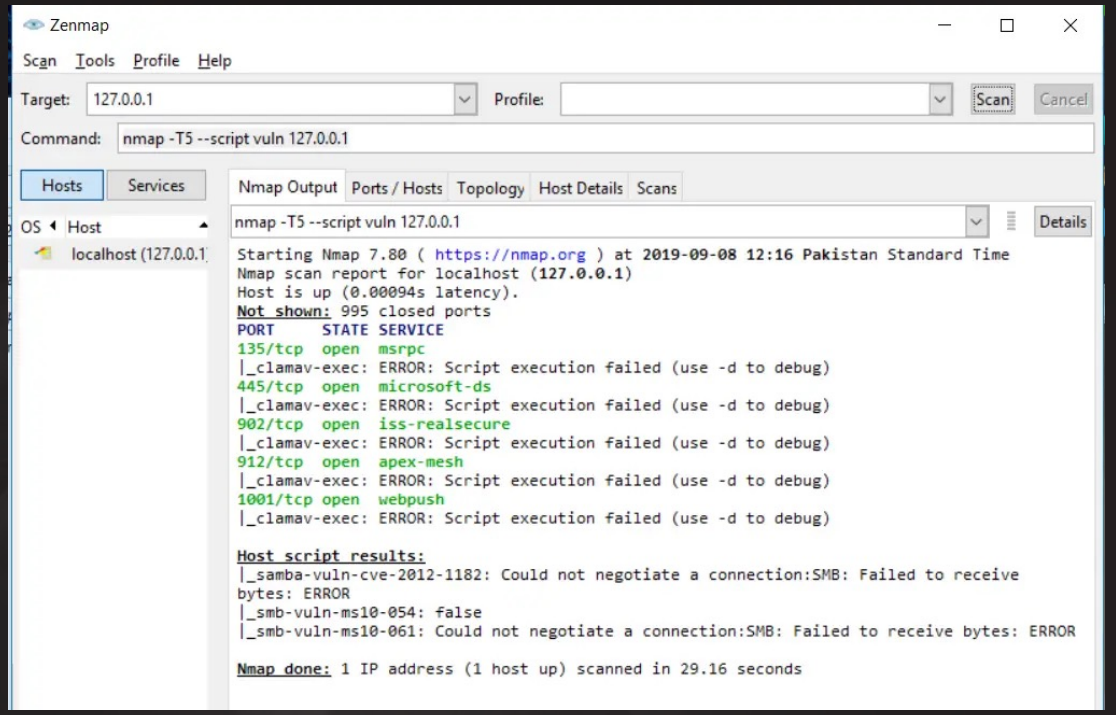
Alinet

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**



https://nmap.org

Alinet

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

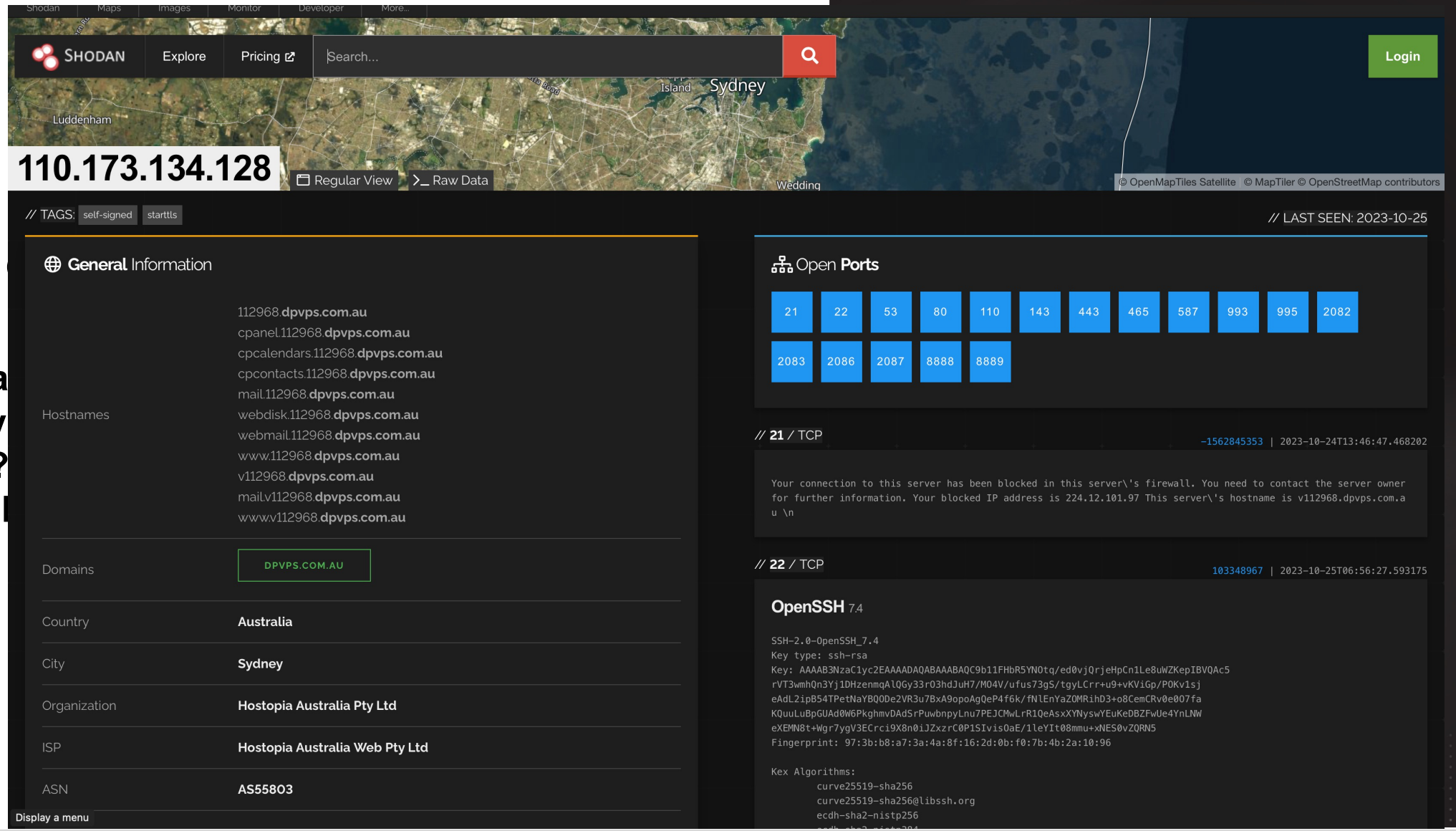
https://nmap.org

Alinet

Checklist PERIMETR:

Jak

Firewa
služby
světa?
kterýcl



Alinet

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

Alinet

Jak chráníte per

**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."
Display a menu 20-	4.3 The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy

PERIMETR:

né služby

t služeb a jejich verze

sti

Alinet

Kolik to stojí?

Alinet

Kolik to stojí?

Ceník:

- ✓ Kolik stojí aktualizace OS serverů a stanic?

Alinet

Kolik to stojí?

Ceník:

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

Alinet CZ s.r.o. Pod Hájkem 406/1a, Praha 8, 180 00, CZ

mobil: +420 774 077 108 **e-mail:** info@alinet.cz **web:** www.alinet.cz

Alinet

Kolik to stojí?

Ceník:

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

Alinet CZ s.r.o. Pod Hájkem 406/1a, Praha 8, 180 00, CZ

mobil: +420 774 077 108 **e-mail:** info@alinet.cz **web:** www.alinet.cz

Alinet

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?

Alinet CZ s.r.o. Pod Hájkem 406/1a, Praha 8, 180 00, CZ

mobil: +420 774 077 108 **e-mail:** info@alinet.cz **web:** www.alinet.cz

Alinet

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?

Alinet CZ s.r.o. Pod Hájkem 406/1a, Praha 8, 180 00, CZ

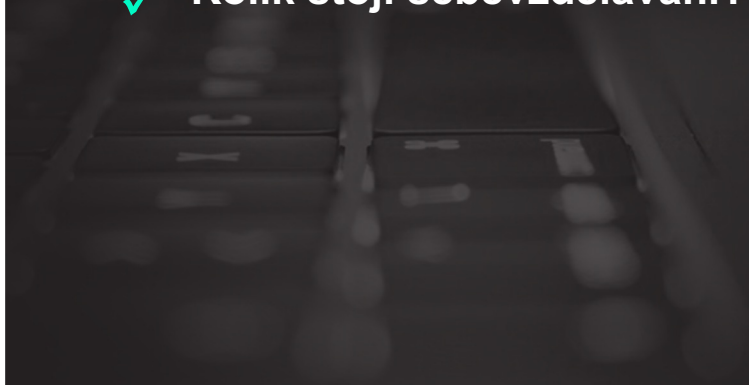
mobil: +420 774 077 108 **e-mail:** info@alinet.cz **web:** www.alinet.cz

Alinet

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?



Alinet CZ s.r.o. Pod Hájkem 406/1a, Praha 8, 180 00, CZ

mobil: +420 774 077 108 **e-mail:** info@alinet.cz **web:** www.alinet.cz

Alinet

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 CZ s.r.o. Pod Hájkem 406/1a, Praha 8, 180 00, CZ

mobil: +420 774 077 108 **e-mail:** info@alinet.cz **web:** www.alinet.cz

Alinet

Cyber Security, **Ransomware Incident Response**

Jakub Alimov

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