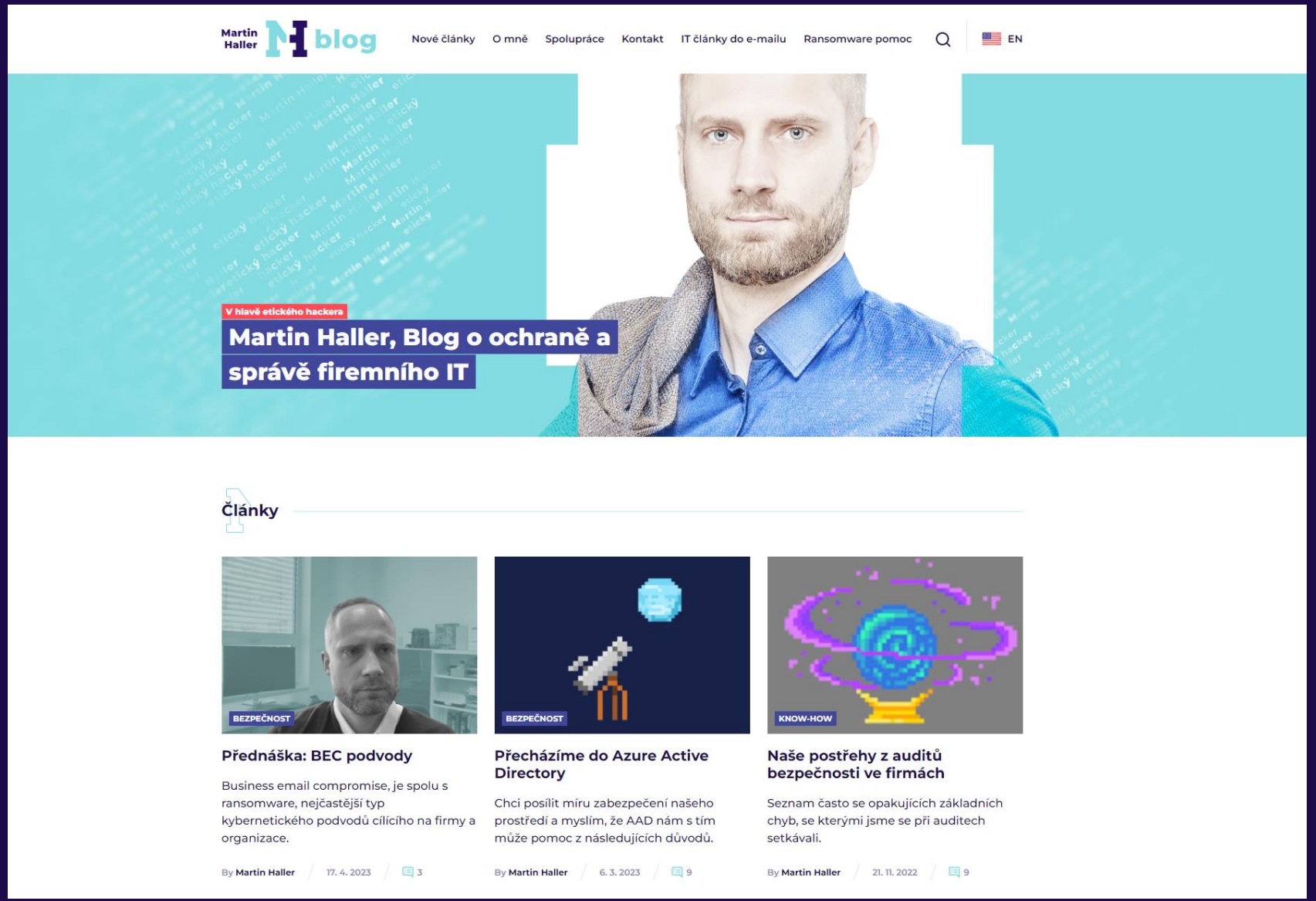
# Martin Haller

## ⟨Jakých bylo posledních 12 měsíců v kybernetické bezpečnosti⟩

PATRON ⟨IT⟩ OCHRANA A SPRÁVA SÍTÍ


Martin Haller blog
Nové články
O mně
Spolupráce
Kontakt
IT články do e-mailu
Ransomware pomoc
EN
V hlavě etického hackera
Martin Haller, Blog o ochraně a správě firemního IT
Články
BEZPEČNOST
Přednáška: BEC podvody
Business email compromise, je spolu s ransomware, nejčastější typ kybernetického podvodů cílícího na firmy a organizace.
By Martin Haller / 17. 4. 2023 / 3
BEZPEČNOST
Přecházíme do Azure Active Directory
Chci posílit míru zabezpečení našeho prostředí a myslím, že AAD nám s tím může pomoc z následujících důvodů.
By Martin Haller / 6. 3. 2023 / 9
KNOW-HOW
Naše postřehy z auditů bezpečnosti ve firmách
Seznam často se opakujících základních chyb, se kterými jsme se při auditech setkávali.
By Martin Haller / 21. 11. 2022 / 9

# Proč je obnova po ransomware utrpení

# Trendy co pozorujeme

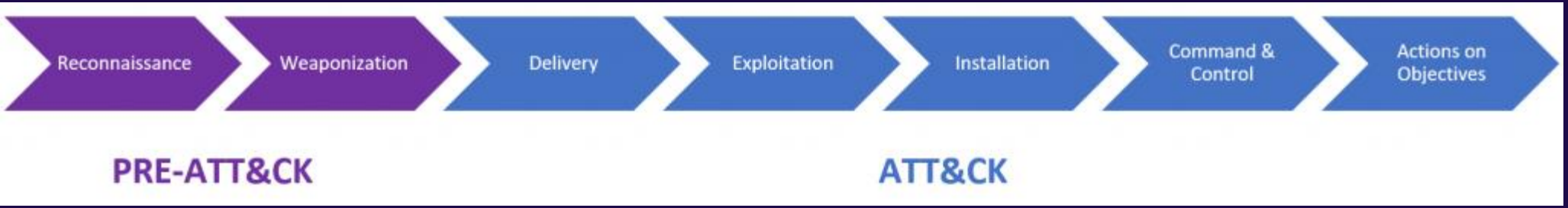
» Útoky začínají až dlouhou dobu po kompromitaci

» Incident response založený na pocitech

» Svět z médií vypadá jinak, než jak jej vidíme my

# Útoky začínají až dlouhou dobu po kompromitaci

- Jak dlouho po prvotní kompromitaci?
- Jak se o tom firmy dozví?
- Jak to útočníci dělají?
- Jak je možné zůstat tak dlouho neodhalený?



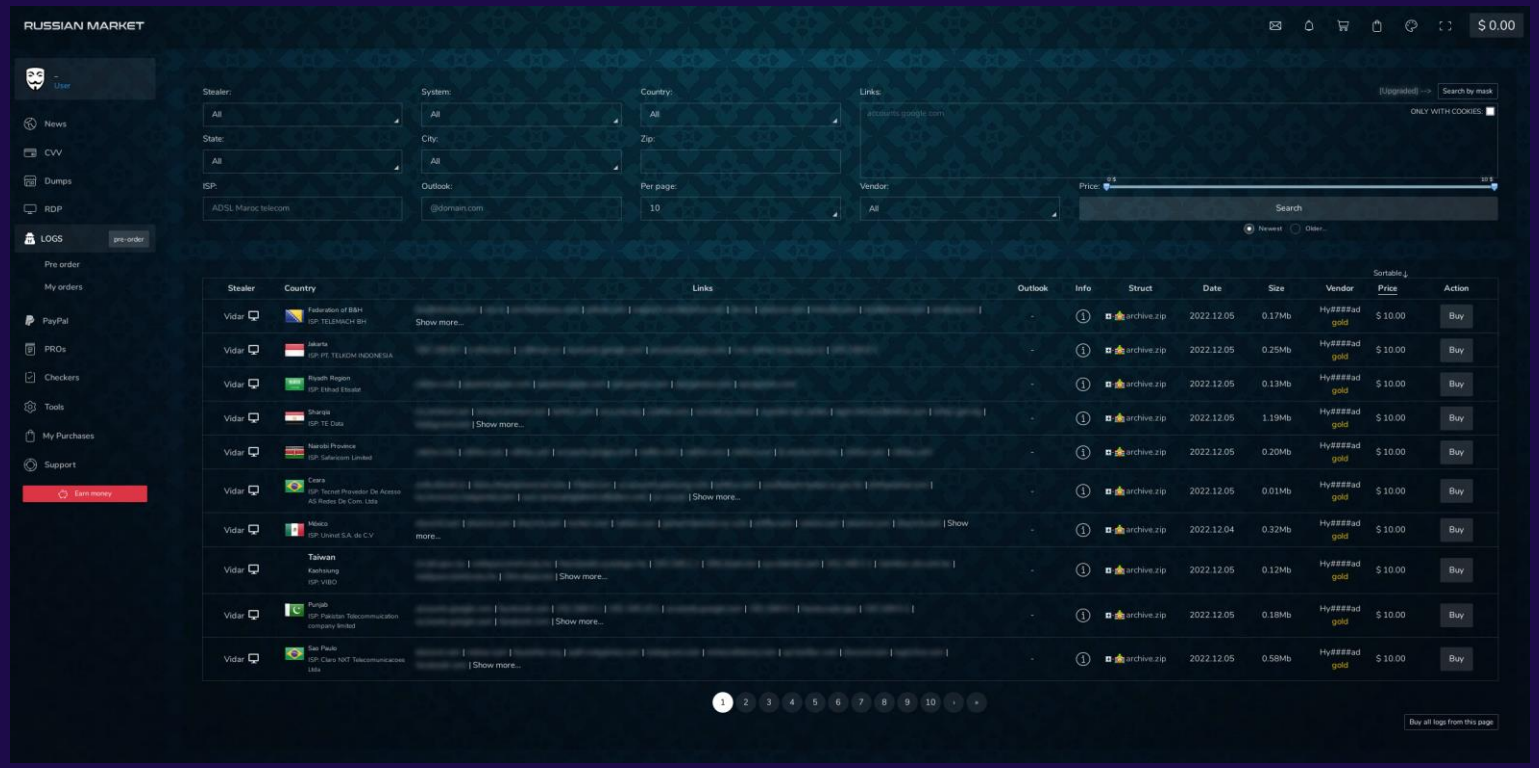

Zdroj: https://www.axians.cz/cs/novinky/jak-probiha-kyberneticky-utok/

# Útoky začínají až dlouhou dobu po kompromitaci

- Na začátku jsou přihlašovací údaje.
- Odkud se vezmou?
- Jak se využijí?

RDP, VPN, RMM, TeamViewer, Microsoft 365,

NAS




Zdroj: https://securityboulevard.com/2023/01/threat-spotlight-top-illicit-sources-to-monitor-in-2023/

# Incident response založený na pocitech

- Proč je obnova po ransomware utrpení
- Čistá instalace, nebo vyčištění současné instalace?

# Potential Actions

- Reset all user account passwords twice (thanks @tazwake)
  - Reset all administrator passwords
  - Reset all service accounts passwords
- Reset (twice – but bear in mind the issues with replication so there's specific guidance on this) the KRBTGT password
- Reset all computer account passwords
- Check the value of the computer account password change value
  - By default, it is 30 days, threat actors can change this to give themselves access using machine hashes for a longer duration. https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/domain-member-maximum-machine-account-password-age
- Reset all LAPS Passwords
- Reset permissions on AdminSDHolders object
- Revoke and re-issue all certificates from ADCS
- Check for malicious scheduled tasks (thanks @SchizoDuckie)
- Check for malicious WMI event filters
- Check for malicious autoruns or other registry-based persistence mechanisms
- Check for utilman style backdoors
- Check for malicious printers/printer drivers (thanks @SchizoDuckie)
- Review Active Directory Delegated access permissions (thank https://twitter.com/@indachtig)
- Rotate ADFS token signing and token decryption certificates (thanks @4n6Bexaminer)
- Check Service Control Manager (SCM) security descriptors (https://docs.microsoft.com/en-us/windows/win32/services/service-security-and-access-rights) (thanks @EricaZeli)
- Check for object changes around initial access/event timescales (thanks @IISResetMe)
- Validate group memberships against known baselines (replication metadata, backup, AD reporting tools/reports etc.) (thanks @IISResetMe)
- Harden Active Directory (look at pingcastle and MITRE) (thanks @MarkSewe)
- Review logon scripts in GPOS and SYSVOL (thanks @CisoDiagonal and A-HAX!)
- Rotate Group Managed Service Accounts (GMSA) (thanks @infosecspy)
- Rotate LAPS credentials
- Review Azure AD/AD Connect (thanks @infosecspy)
- Harden Endpoints
- Update AV
- Deploy EDR
- Deploy SYSMON
- DNS Zone Integrity (Public and Private) (thanks to @jermuv)
- Rote domain trust keys (thanks @DebugPrivilege)
- Review potential RBCD Bakdoors (thanks @DebugPrivilege)
- Review msDsConsistencyGuid attribute of compromised accounts (thanks @DebugPrivilege)
- Check Exchange (easy right?)
- Review accounts for "Key Trust Account Mapping" takeover and reset if required (thanks @nodauf)
  - https://posts.specterops.io/shadow-credentials-abusing-key-trust-account-mapping-for-takeover-8ee1a53566ab
- Review Active Directory Domains and Trusts (thanks @dragon199421)
- Deploy new Domain Controllers (keep existing forest/domain metadata)
- Clear VSS/Backups/Snapshots that are likely to be classed as unsafe (thanks to @Digit4lbytes)

There's also a great blog by Huy here with practical steps to take with LockBit 2.0 as an example:

Practical Guidance for IT Admins to respond after Ransomware attacks | Microsoft 365 Security (m365internals.com)

Zdroj: https://www.pwndefend.com/2021/09/15/post-compromise-active-directory-checklist/

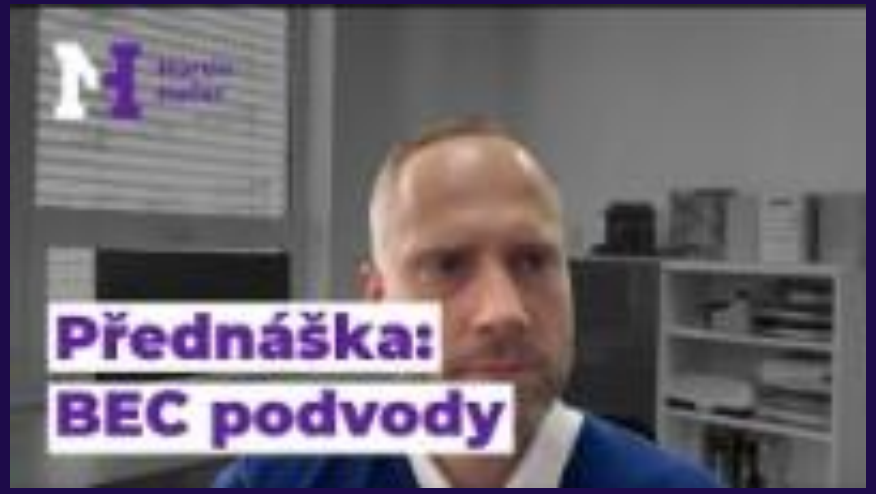
# Incident response založený na pocitech

- Proč je obnova po ransomware utrpení
- Čistá instalace, nebo vyčištění současné instalace?
- Domněnky jsou zbytečné, když se to dá ověřit.
- Když se útočníci vrací
- Mějte komu zavolat

# Svět z médií vypadá jinak

Válka na Ukrajině a strach ze státních akterů

- Zbraně hromadného ničení: NotPetya
- Omezení v lidských zdrojích
- Rozdílné zájmy
- Pro běžné subjekty: finančně motivovaná zločinnost  (ransomware a BEC)



# Svět z médií vypadá jinak

Co sledovat?

» https://martinhaller.cz/wp-content/uploads/2023/06/feedly-security.opml

» https://www.bleepingcomputer.com/

# Dlouhodobí nepřátelé bezpečnosti

- Komplexita, nepřítel bezpečnosti
- Čekání na dokonalé řešení
- Přehlížení celkových nákladů

# Komplexita, nepřítel bezpečnosti

- Co vše máme v síti?
- Sledovat release notes
- Provádět aktualizace
- Udržovat konfiguraci
- Zaučování nových správců

# Komplexita, nepřítel bezpečnosti

Příklady:

- Firewall (viditelnost na DC)
- Zálohovací SW
- Active Directory
- Azure Active Directory
- Tier-0 systémy

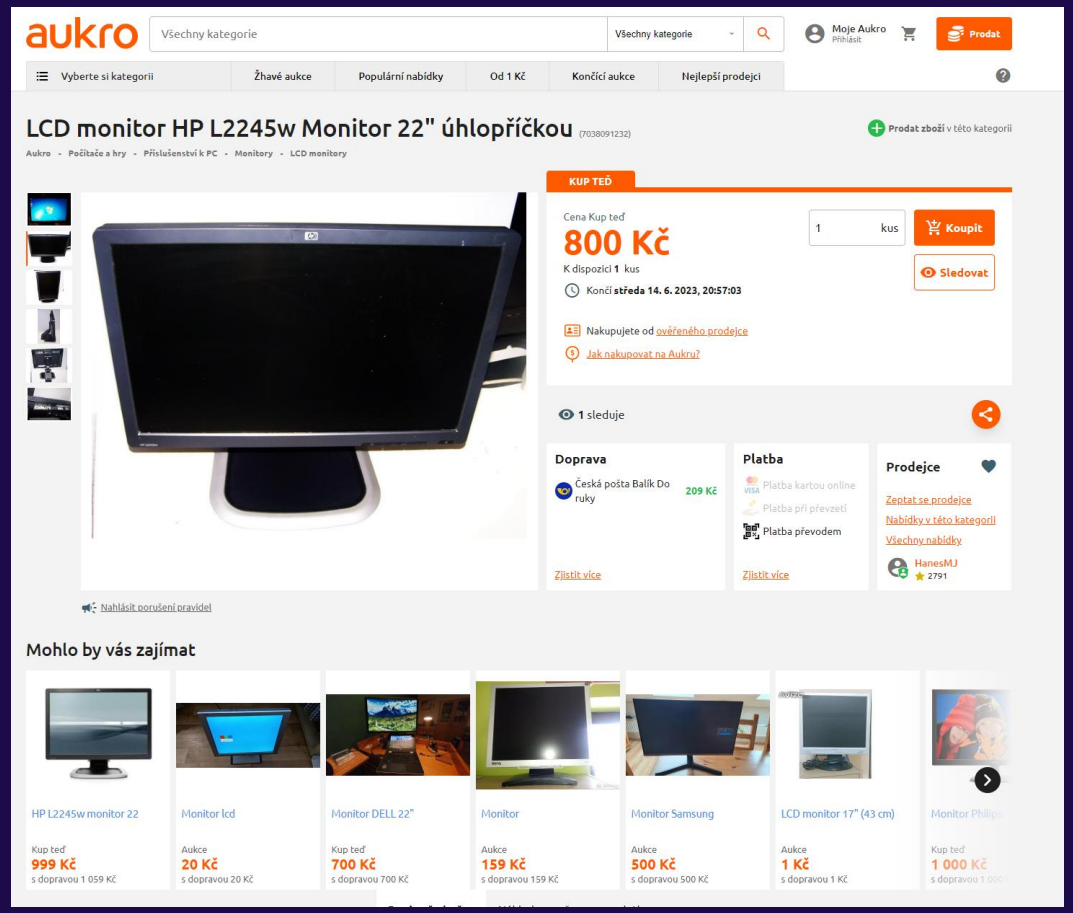
Backup servery, DCs, Hyper-V/VMware, iDrac, AV/EDR, Azure AD Connect, AD FS, RMM tools, Password managers

# Čekání na dokonalé řešení

- … ale …
- Vše je zpravidla lepší než současný stav
- Kam jsme se za rok posunuli?
- Je potřeba začít krůček po krůčku

# Přehlížení celkových nákladů

- Péče o firemní prostředky jako o rodinný rozpočet.
- Neuvědomování si nákladů času



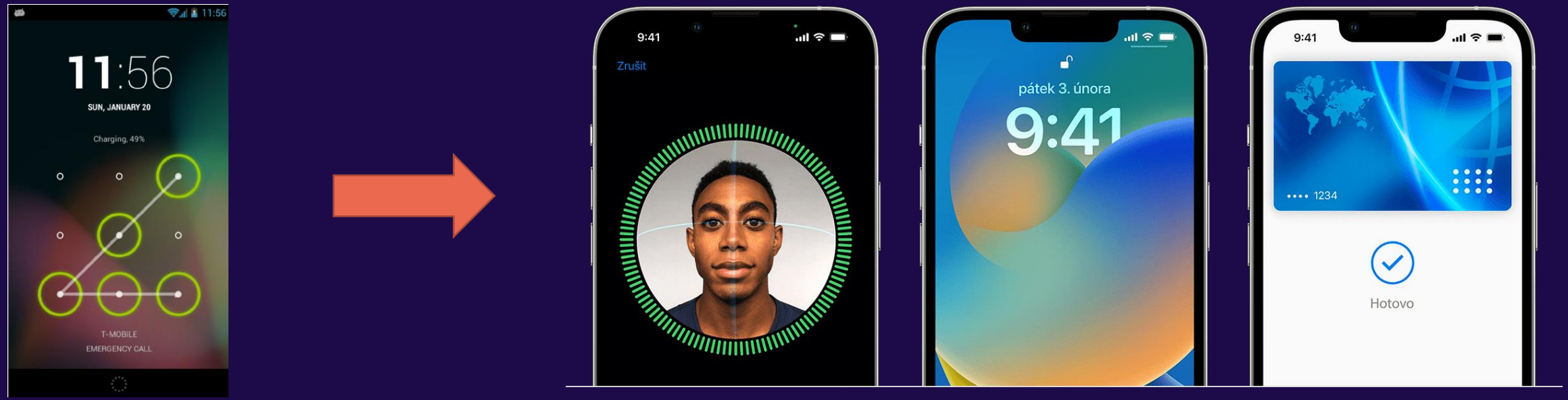
# Jak si prioritizovat práci

# Jak si prioritizovat práci

- Fronta práce je dlouhá
- Každé opatření má své přínosy a náklady
- Náklady = jednorázové (implementace) + pravidelné (údržba)
- Náklady = čas, peníze, omezení / restrikce
- Čas je to co nám většinou chybí
- Byznys plány často přehlíží náklady na IT práci (i HW)
- Co když existují opatření co mají záporné náklady??

# Jak si prioritizovat práci

- Zjednodušení (méně serverů, služeb, centrální správa)
- Delegování (Exchange Online, cloud backup, AWS/Azure)
- Revoluční technologie: biometrické ověřování

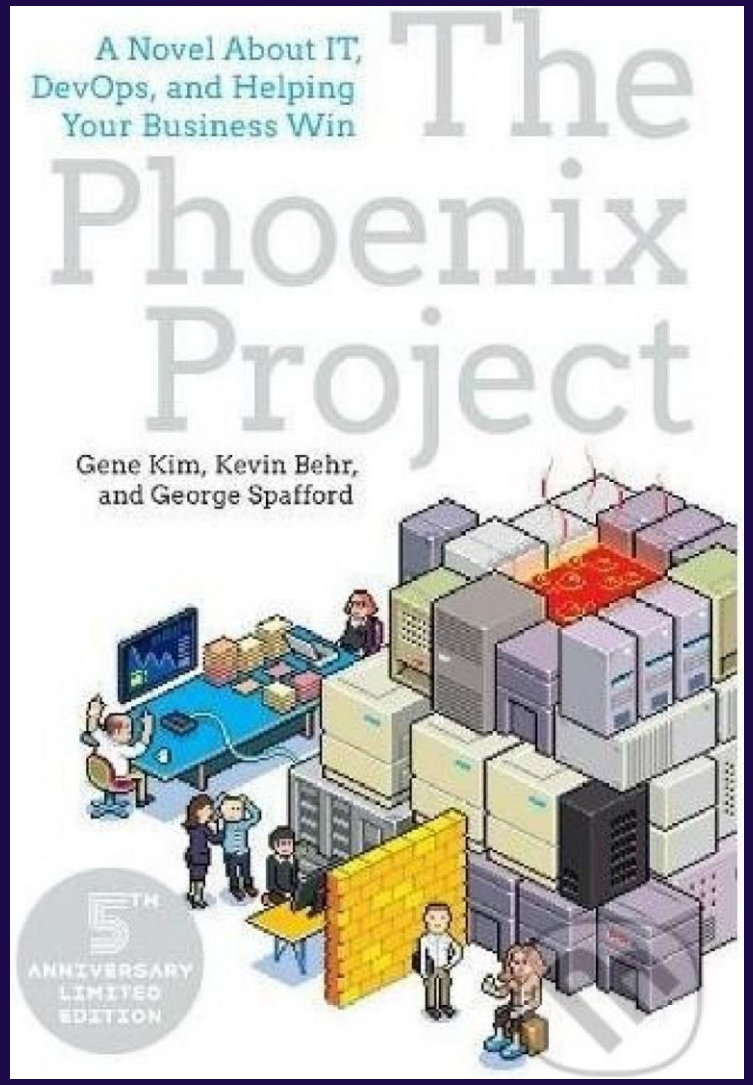


# Jak si prioritizovat práci

## The Phoenix Project:

A Novel about It, Devops, and Helping Your Business Win

“Every person involved in a failed IT project should be forced to read this book.” - TIM O'REILLY, Founder & CEO of O'Reilly Media “The Phoenix Project is a must read for business and IT executives who are struggling with the growing complexity of IT.” - JIM WHITEHURST, President and CEO, Red Hat, Inc.

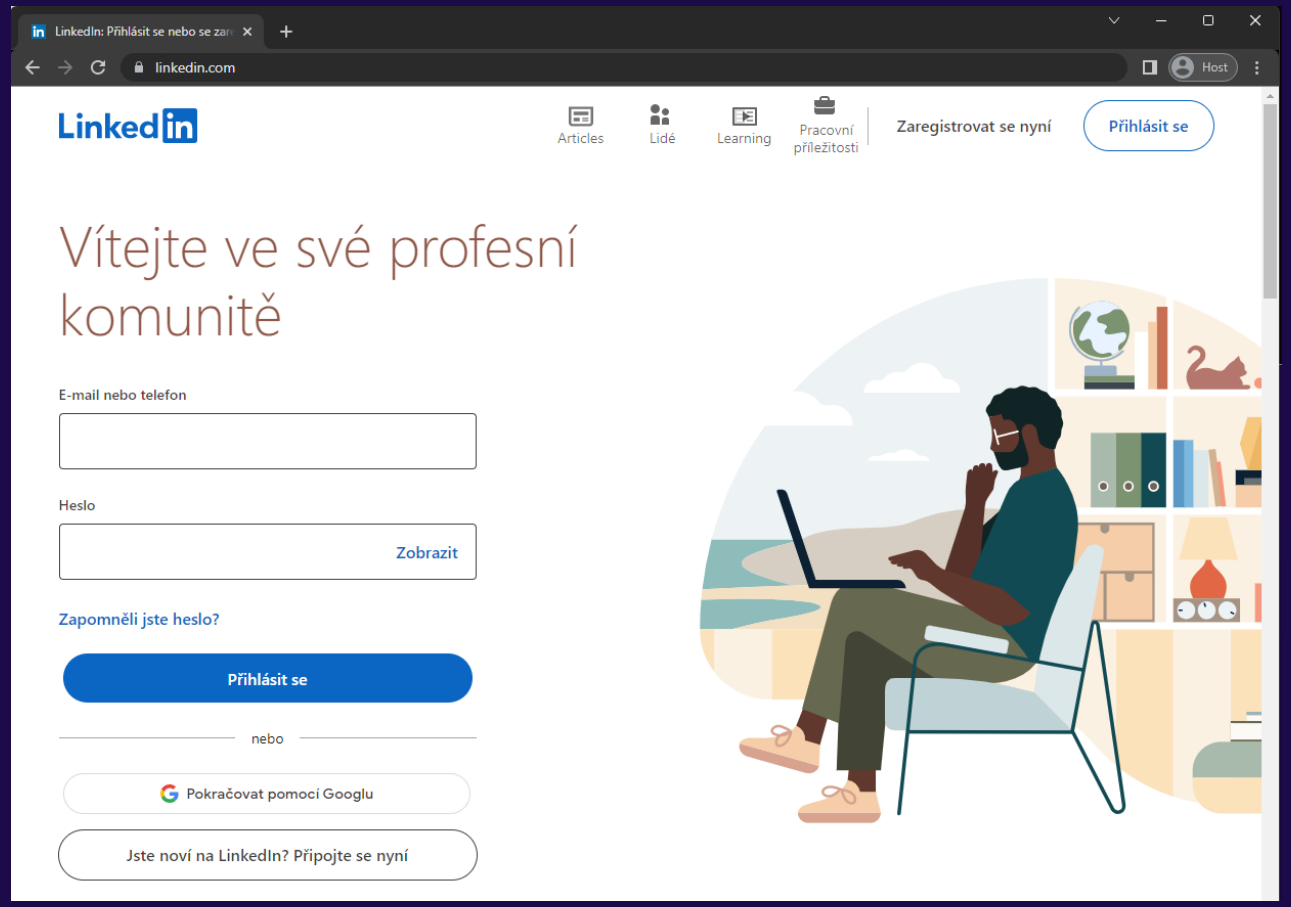


# Technologie budoucnosti

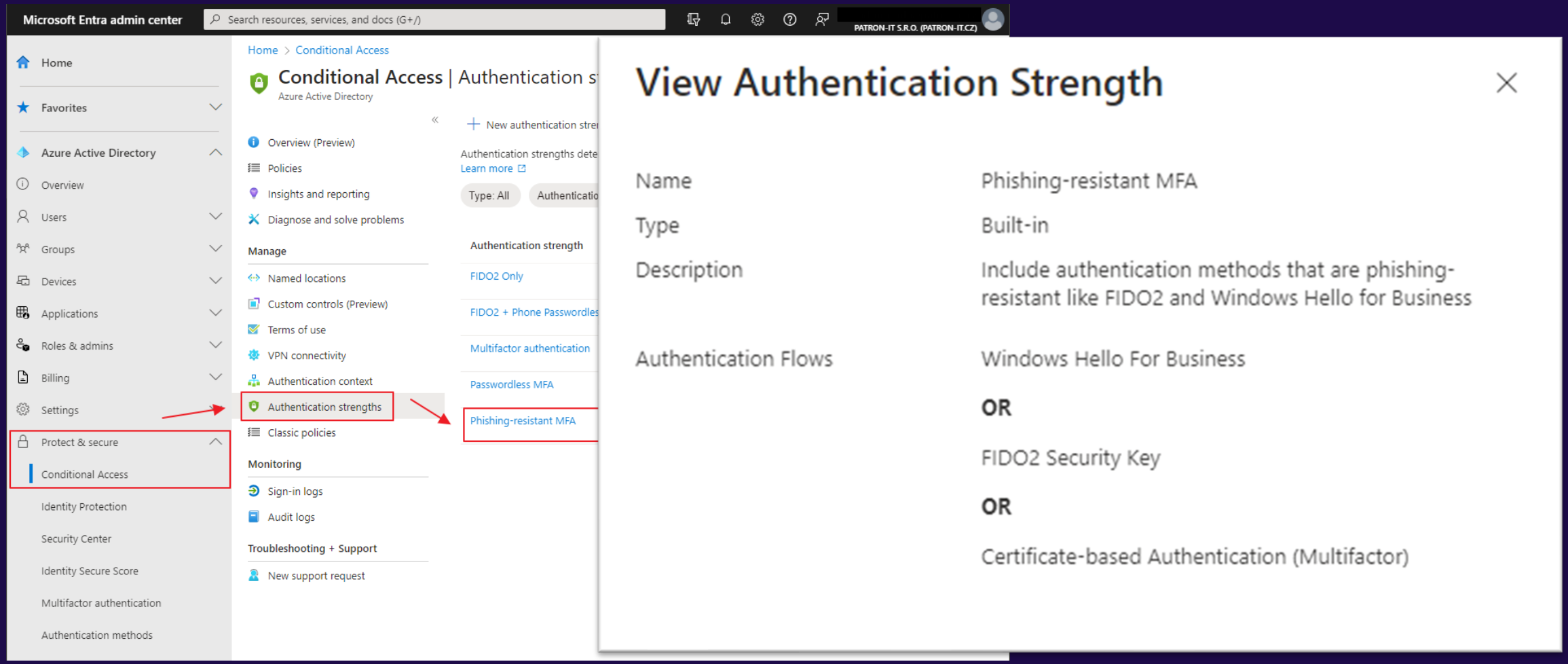
- Identity providers (Azure Active Directory)
- FIDO2 / PassKeys

# Identity providers

- Nic nového pod sluncem: MojeID, Facebook, Apple ID, Google, Microsoft, Active Directory, AD FS
- Azure Active Directory
  - Jedna metoda ověřování
  - Logy na jednom místě
  - Conditional Access
  - Jednoduchý onboarding / offboarding



# FIDO2 / PassKeys



# FIDO2

- Phishing-resistant MFA?
- Snadnost používání
- Nejvyšší míra zabezpečení

Nevýhody:

- Platformní podpora
- Potřeba více klíčů
- Kapacitní omezení

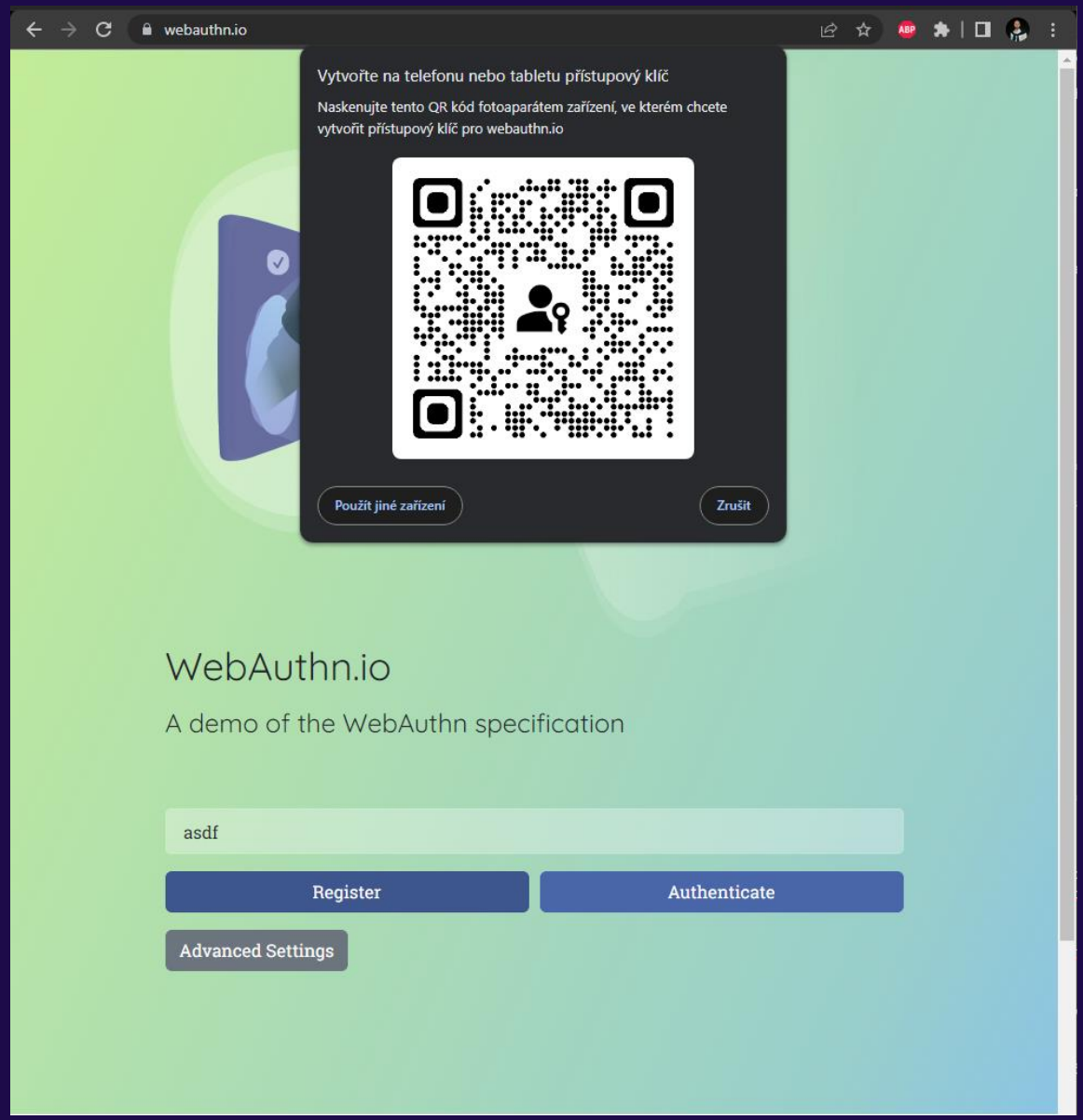
Zdroj: https://www.kensington.com/

# PassKeys

- Budoucnost hesel
- Snadnost používání
- Synchronizace mezi zařízeními
- Možnost sdílet
- Platformní podpora

Nevýhody:

- Menší úroveň zabezpečení než HW klíče (pro uživatele však více než dostatečné!!)



# PassKeys

» Phishing resistant vůči cizím QR kódům

## Chrome's passkey support summary

| Operating systems | Android | macOS | iOS/iPadOS | Windows | Linux |
|---|---|---|---|---|---|
| Local user verification | ✓ | ✓ | ✓ | ✓ | ⊘ |
| Passkey sync | ✓ | 🕒[1] | ✓[1] | ⊘[3] | ⊘ |
| Autofill | ✓ | ✓ | ✓ | ✓[2] | ⊘ |
| Can sign in with a phone | 🕒 | ✓ | ✓ | ✓ | ✓ |

✓ : Supported, 🕒: Planned, ⊘ : No plans

[1]: Syncs with iCloud Keychain [2]: Requires Windows 11 22H2 [3]: Depends on Windows Hello

Zdroj: https://developers.google.com/identity/passkeys/supported-environments

# Děkuji za ⟨pozornost⟩