



Martin Haller

《 Jakých bylo posledních 12
měsíců v kybernetické
bezpečnosti 》

PATRON 《IT》 OCHRANA
A SPRÁVA SÍTÍ

V hlavě etického hackera

Martin Haller, Blog o ochraně a správě firemního IT

Články



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



Přecházíme do Azure Active Directory

Chci posílit míru zabezpečení našeho prostředí a myslím, že AAD nám s tím může pomoci z následujících důvodů.

By Martin Haller / 6. 3. 2023 /  9



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

The screenshot shows the 'RUSSIAN MARKET' website interface. At the top, there are search filters for Stealer, System, Country, State, City, Zip, ISP, Outlook, and Vendor. A price slider is set to \$0.00. Below the filters is a table listing various stolen data items for sale. Each item includes a 'Stealer' name, a 'Country' flag, a 'Links' column, an 'Outlook' column, an 'Info' column, a 'Struct' column, a 'Date' column, a 'Size' column, a 'Vendor' column, a 'Price' column, and an 'Action' column.

Stealer	Country	Links	Outlook	Info	Struct	Date	Size	Vendor	Price	Action
Vidar	Federation of BH1 ISP: TELEMACH BH	Show more...	-	1	archive.zip	2022.12.05	0.17Mb	Hy####ad gold	\$ 10.00	Buy
Vidar	Jakarta ISP: PT. TELKOM INDONESIA	Show more...	-	1	archive.zip	2022.12.05	0.25Mb	Hy####ad gold	\$ 10.00	Buy
Vidar	Pratih Region ISP: Etihad Stealer	Show more...	-	1	archive.zip	2022.12.05	0.13Mb	Hy####ad gold	\$ 10.00	Buy
Vidar	Shiraz ISP: TE Data	Show more...	-	1	archive.zip	2022.12.05	1.19Mb	Hy####ad gold	\$ 10.00	Buy
Vidar	Narada Province ISP: Subcon Limited	Show more...	-	1	archive.zip	2022.12.05	0.20Mb	Hy####ad gold	\$ 10.00	Buy
Vidar	Creta ISP: Netel Proxifier Dr. Alessio AS Redes De Com. Ltda	Show more...	-	1	archive.zip	2022.12.05	0.01Mb	Hy####ad gold	\$ 10.00	Buy
Vidar	Milao ISP: Univel S.A. de C.V.	Show more...	-	1	archive.zip	2022.12.04	0.32Mb	Hy####ad gold	\$ 10.00	Buy
Vidar	Taiwan Kashberg ISP: VIBCO	Show more...	-	1	archive.zip	2022.12.05	0.12Mb	Hy####ad gold	\$ 10.00	Buy
Vidar	Puerto Rico ISP: Paraiso Telecommunication company limited	Show more...	-	1	archive.zip	2022.12.05	0.18Mb	Hy####ad gold	\$ 10.00	Buy
Vidar	Sao Paulo ISP: Claro NBT Telecomunicacoes Ltda	Show more...	-	1	archive.zip	2022.12.05	0.58Mb	Hy####ad gold	\$ 10.00	Buy

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)
- Rotate domain trust keys (thanks @DebugPrivilege)
- Review potential RBCD Backdoors (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/>

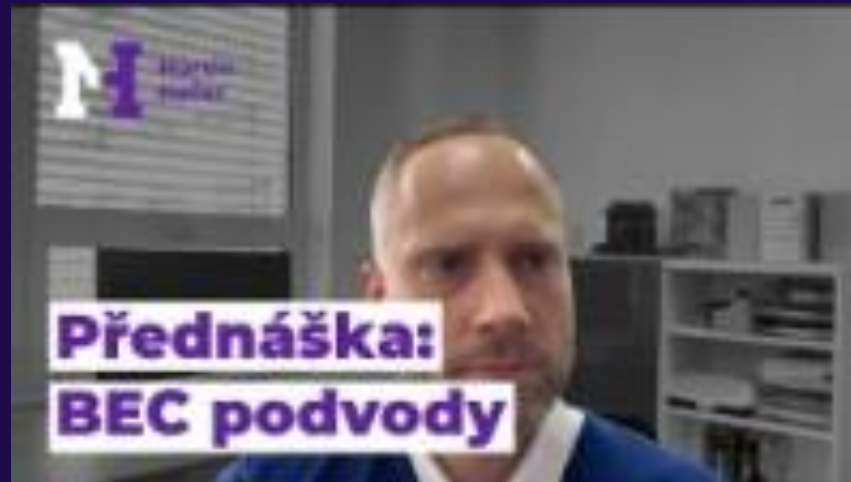
Incident response založený na pocitech

- » 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

The screenshot shows the aukro.com website interface. At the top, there is a navigation bar with the aukro logo, search bars, and user account options. The main content area features a product listing for an "LCD monitor HP L2245w Monitor 22" úhlopříčkou". The product image is a large black monitor on a stand. To the right of the image, the price is listed as "Cena Kup teď 800 Kč" with a "KUP TĚD" button. Below the price, there is information about availability ("K dispozici 1 kus") and the auction end time ("Končí středa 14. 6. 2023, 20:57:03"). There are also buttons for "Koupit" and "Sledovat". Below the main product, there are sections for "Doprava" (Česká pošta Balík Do ruky, 209 Kč), "Platba" (Platba kartou online, Platba při převzetí, Platba převodem), and "Prodejce" (HanesMJ, 2791). At the bottom, there is a "Mohlo by vás zajímat" section with several smaller product listings, each with a small image and price information.

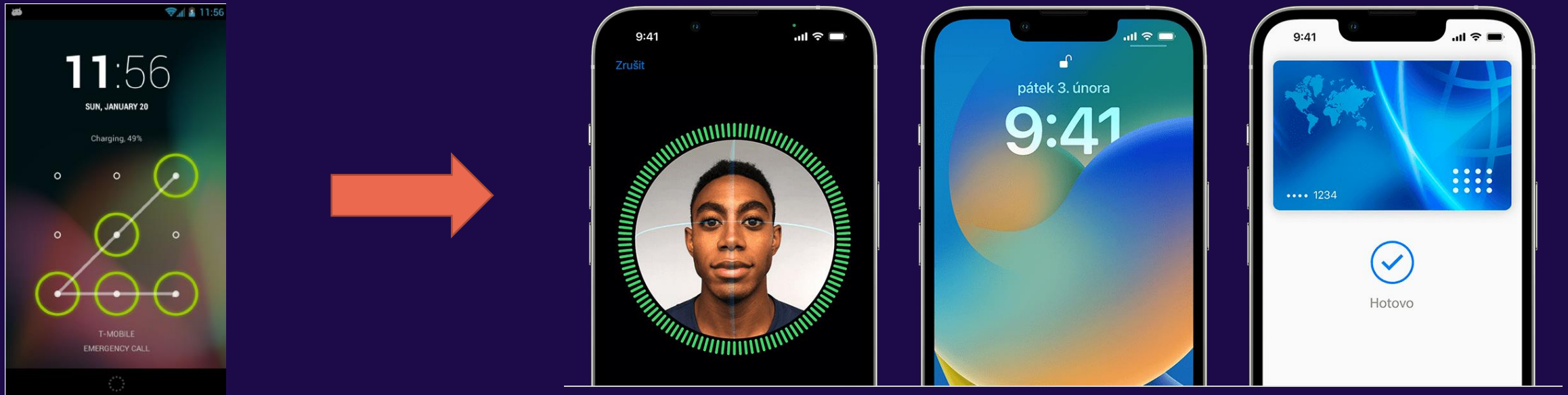
Jak si prioritizovat práci

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

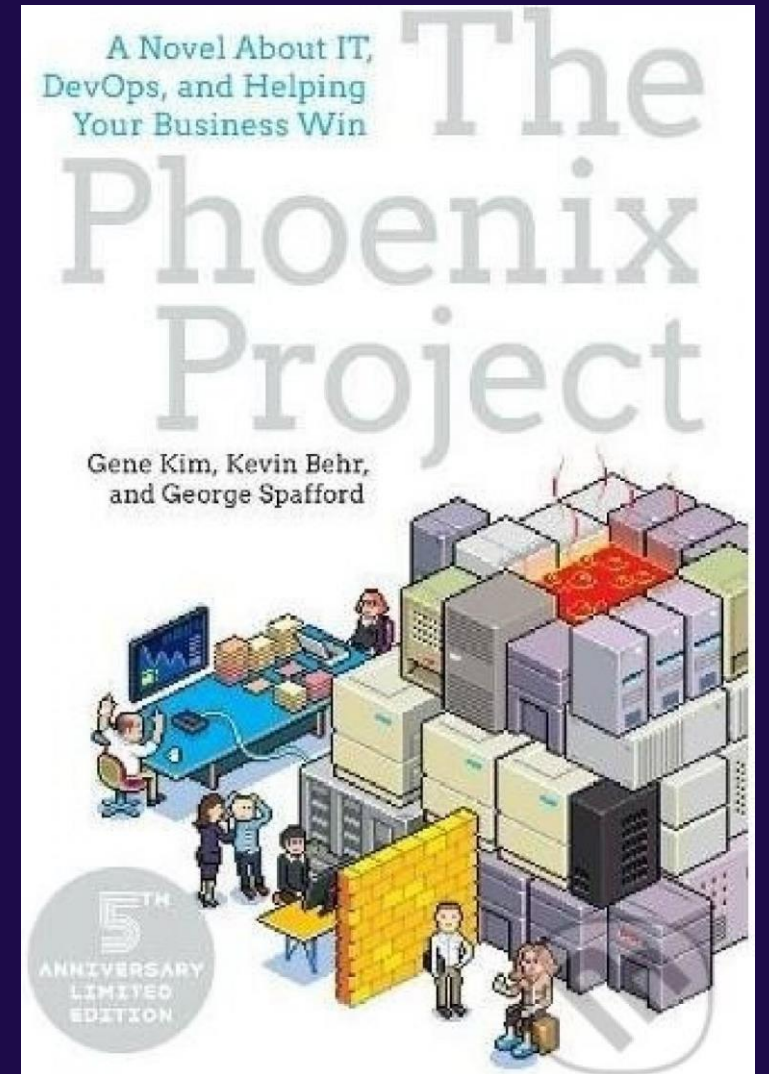


Jak si prioritizovat práci

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.

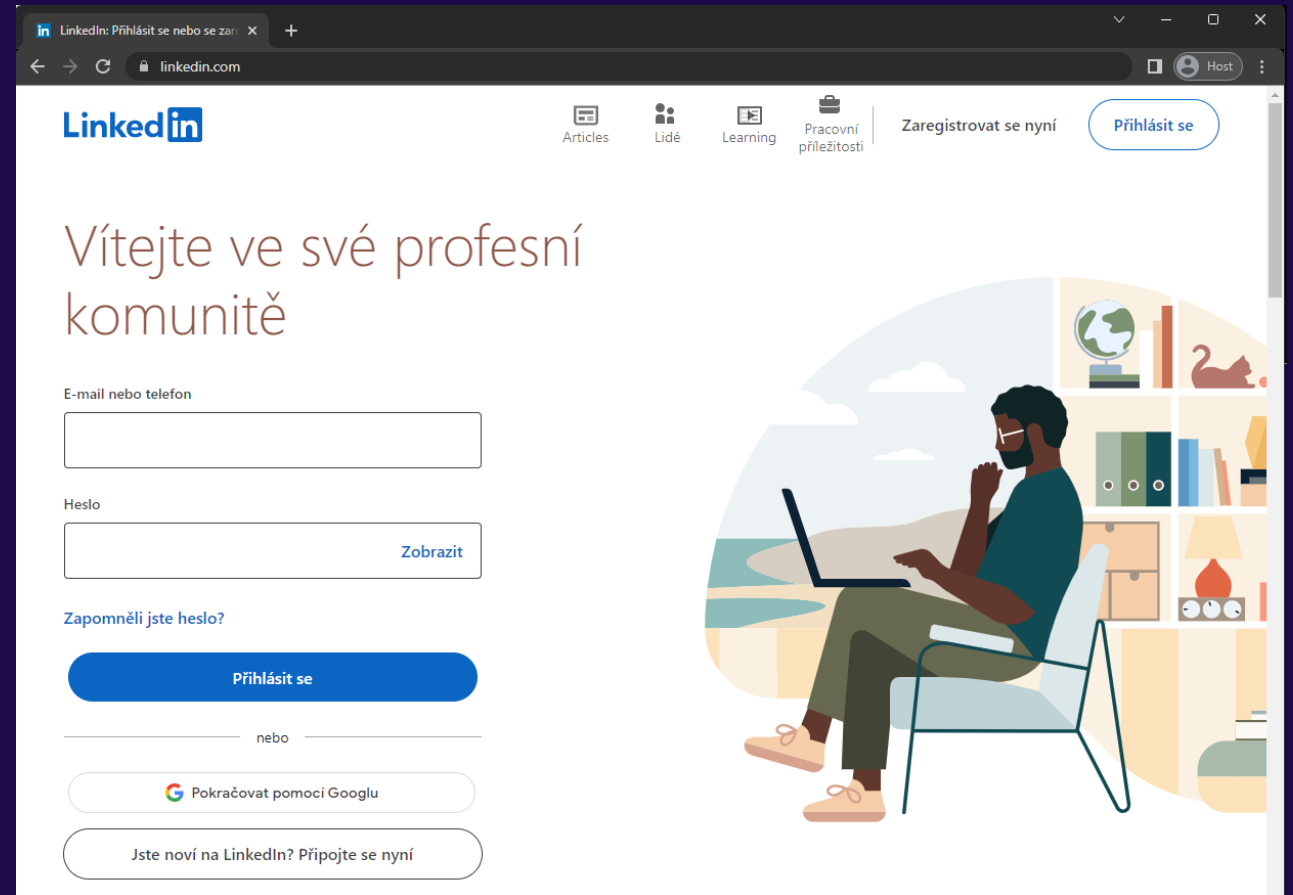


- » Identity providers (Azure Active Directory)
- » FIDO2 / PassKeys

Technologie budoucnosti

Identity providers

- » Nic nového pod sluncem: MojID, 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

The screenshot shows the Microsoft Entra admin center interface. The left-hand navigation pane is open to 'Protect & secure' > 'Conditional Access'. The main content area displays the 'Authentication strengths' configuration page. A red box highlights the 'Authentication strengths' link in the left pane, and another red box highlights the 'Phishing-resistant MFA' link in the main content area. A third red box highlights the 'Authentication strength' section in the main content area, which lists several options: 'FIDO2 Only', 'FIDO2 + Phone Passwordless', 'Multifactor authentication', 'Passwordless MFA', and 'Phishing-resistant MFA'. A modal window titled 'View Authentication Strength' is open on the right, showing details for the 'Phishing-resistant MFA' strength.

Property	Value
Name	Phishing-resistant MFA
Type	Built-in
Description	Include authentication methods that are phishing-resistant like FIDO2 and Windows Hello for Business
Authentication Flows	Windows Hello For Business OR FIDO2 Security Key OR Certificate-based Authentication (Multifactor)

FIDO2

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

Nevýhody:

- » Platformní podpora
- » Potřeba více klíčů
- » Kapacitní omezení



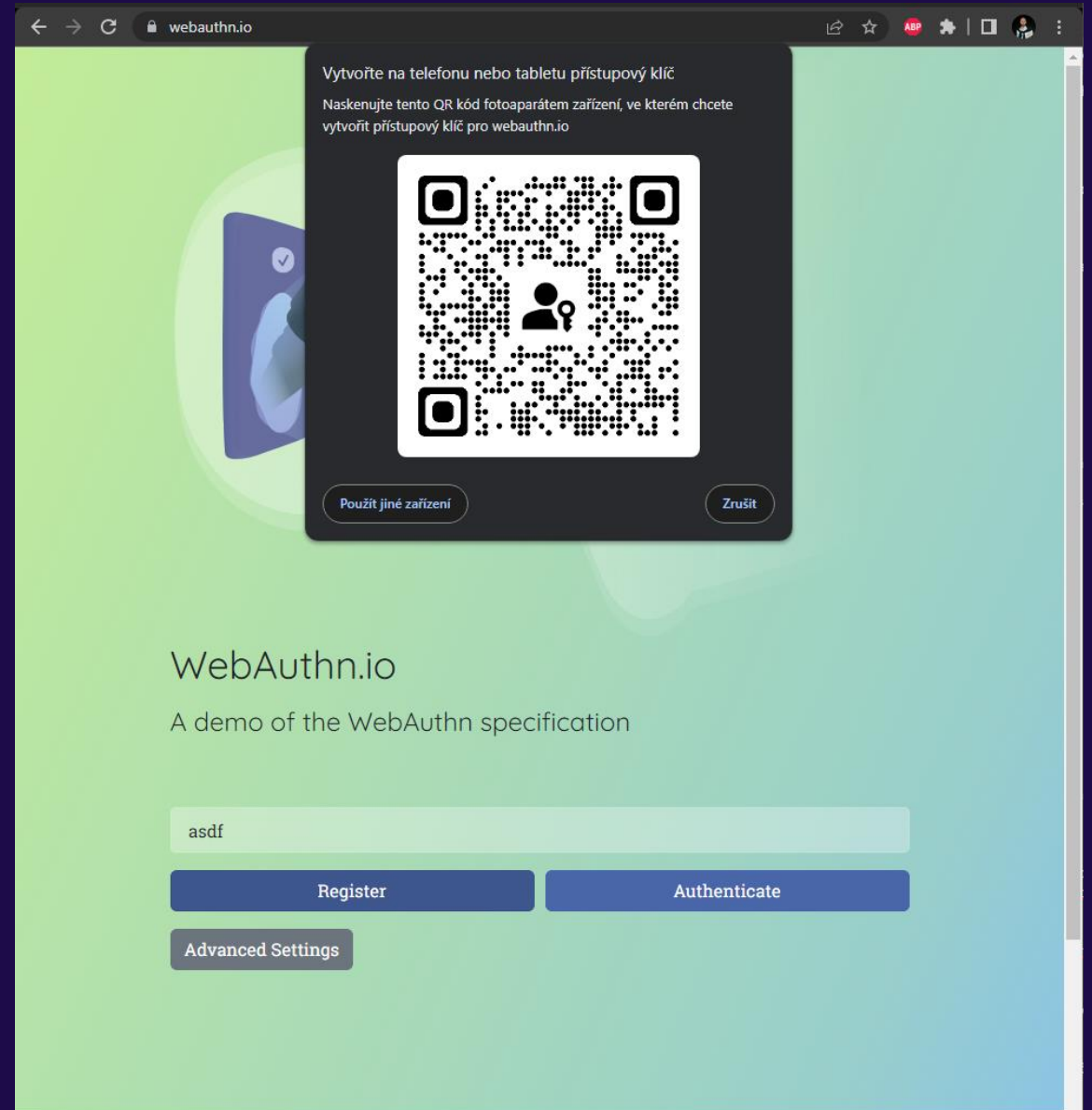
Zdroj: <https://www.kensington.com/>

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⟩