Základy kybernetické bezpečnosti
Bezpečnost a analýza dat

Ing. Vladimír Lazecký
vladimir.lazecky@viavis.cz

VIAVIS střežíme podstatné

Dovolte, abych se představil

- **Ing. Vladimír Lazecký**
  - CEO společnosti VIAVIS a.s.
  - V oboru od roku 1994

- **VIAVIS** je nezávislá konzultační společnost
  - Ochrana a bezpečnost informací, integrovaná bezpečnost
  - Řešení bezpečnostních incidentů
  - Kyber bezpečnost
  - Soudní znalci
  - Bezpečnostní management

Základní témata předmětu

- Motivace
- Základní pojmy a principy
- Informační systémy
- Systematické řešení – technická a organizační opatření
- Incident management, BCP
- Trendy v oblasti informační a kybernetické bezpečnosti

Cíl přednášek

- Ukázat reálný obsah pojmu „**kybernetická bezpečnost**“
  - Kybernetická nebo informační bezpečnost?
  - Je více bezpečností?
  - Pouze téma odborníků?
  - Jaká je reálná role státu

- Role informační bezpečnosti v současném světě
  - Bezpečnost x svoboda

- Předat alespoň základní nadhled nad obor
  - Pochopení problému a principů
  - Korigovat nereálné představy

Kybernetická bezpečnost – pojmy, pojmy, pojmy…

- **Kybernetika**:
  - *Je věda, která se zabývá obecnými principy řízení a přenosu informací ve strojích, živých organismech a společenstvích* (www.wikipedia.cz)

- **Kybernetická bezpečnost (Cyber Security)**
  - *Souhrn právních, organizačních, technických a vzdělávacích prostředků směřujících k zajištění ochrany kybernetického prostoru*
    - http://www.cybersecurity.cz

- **Kybernetický prostor (Cyberspace)**
  - *Digitální prostředí umožňující vznik, zpracování a výměnu informací tvořené informačními systémy, službami a sítěmi elektronických komunikací*
    - http://www.cybersecurity.cz

Kybernetická bezpečnost – zatím jen motivace

- **Kybernetický útok (Cyber Attack)**
  - *Útok na IT infrastrukturu za účelem způsobit poškození a získat citlivé či strategicky důležité informace.*

  - Tyto definice **nejsou úplně přesné**:
    - Kybernetická bezpečnost je stále bezpečností
    - Nejde pouze o útoky na IT infrastrukturu – velká komplexnost
    - Nebezpečí chápání zodpovědnosti uživatelů:
      - *„O to se stará ajťák, tomu nerozumím“*
      - *„Jde o problém státu, mne se to netýká“*
      - *„Nemám co tajit, kdo by na mne útočil“*

Motivace – proč bezpečnost

- **Důvodem pro ochranu čehokoli je hodnota**
  - Pokud je něco bezcenné, nemá smysl to chránit
  - Každá hodnota sebou nese riziko
  - S růstem hodnoty roste riziko incidentu

- **Bezpečnost – existuje jich více?**
  - Dá se problém zúžit jen na kybernetickou bezpečnost?
  - Je kybernetická bezpečnost problém pouze odborníků?

Něco málo historie

- **Informace vždy hrály rozhodující úlohu**:
  - Války – převaha informací byla vyšší hodnotou než vojenská
  - Vlády – ekonomická politika, mezinárodní politika, bezpečnostní politika
  - Soukromý sektor – průmyslová špionáž
  - Marketing – Apple, automotive, politické strany

- **Nový trend – informační boj, hybridní hrozby**
  - Útoky na fakta a jejich ověřitelnost – fake news
  - Na základě špatných dat nelze učinit správná rozhodnutí
  - Mediální realita, postpravda, relativizace
  - Více mimoběžných realit
  - Jak lze ověřovat realitu?

Něco málo historie

- Neoprávněné získání informací – fyzická špionáž
- Manipulace s informacemi
- Zamezení přístupu k informacím
  - Pokusy se děly vždy
  - Globální prostor získání informací usnadňuje (kyber prostor)
- Dopady incidentů:
  - Ovlivnění životů lidí
  - Politické dopady
  - Ekonomické dopady
  - Narušení společnosti
- **Nepoměr mezi náklady na incident a jeho dopady**
  - **Vysoká efektivita**

Něco málo historie

- Ochrana informací:
  - Snaha o ochranu tady byla vždy (neviditelný inkoust…)
- Dnes:
  - Radikálně se mění technologie
  - Lidská mentalita se nemění
  - Chybí bezpečnostní zkušenost
  - Nevnímání rizik
  - Závislost na způsobu zpracování informací
  - Rostou dopady incidentů – globální dopady
  - Základní metody ochrany zůstávají - technické x organizační x hodnotové

Informační závislost extrémně roste

Něco málo historie

- Rozvoj IT přinesl kvalitativní změnu
  - Rozvoj Internetu – 90. léta:
    - Velmi snadný přístup k informacím
    - Rychlost komunikace
    - Nikdo nebyl připraven na nový typ hrozeb
    - **Ochrana je reaktivní**

- Bezpečnost IT systémů – historicky se jim věnovala malá pozornost
- Změna od roku 2000 – první publikované vážné bezpečnostní incidenty
- Začal převažovat zájem o IT bezpečnost
- „Bláznivé“ investice do IT ochrany

- Ochrana soukromí?

Proč internet?

- **Proč se stáváme závislými?**
  - Veřejná správa
  - Business – B2B, B2C…
  - Kritická infrastruktura
  - Sociální sítě
  - Cloud
  - Internet věcí
  - Technologie řídí životy

- Vidíte důvod?

Všimli jste si, jak se změnil svět?

- Jak je snadné „ukrást“ cenou informaci?
  - Veletrhy kdysi x internet nyní
  - Jak je obtížné chránit drahé know how?
- Dříve:
  - Úspěch byl podmíněn nápadem, rychlostí, šikovností, na realizaci nápadu byl čas
  - Existoval lokální business – globální bariéry
  - Náklady na rozjezd podnikání
- Nyní:
  - „*Úspěšní se nápady inspirují, bohatí nápady kradou*…“ (www.ihned.cz)

Nové problémy dneška

- **Ochrana osobnosti a svobody jednotlivce**
  - Monitoring „od kolébky do hrobu“
    - Telekomunikační operátoři
    - IS veřejné a státní správy, registry
    - Kamerové systémy
    - Platební systémy, EET, IoT…
  - Bezpečnostní systémy
    - Terorismus
    - Infrastruktura IS – využívá internet
  - Dobrovolné „uložiště“ soukromých informací:
    - Sociální sítě…
  - Kde je hranice?
  - Dá se ochrana osobnosti vynutit zákonem?
  - Co lze dělat s informací umístěnou na internet?

Je „kybernetická bezpečnost“ pouze problém IT nebo internetu?

- **Společnost měla nápad – jednoduchá technologie s úsporami 80% proti cenám konkurence**
  - Do vývoje investovala nemalé prostředky
  - Na vývoji se podíleli externisté
  - Mezi externisty a společností neexistovaly objednávky a smlouvy specifikující předmět plnění
  - Komunikace, vše probíhalo elektronicky, volně, nešifrovaně
  - Externisté samostatně registrovali průmyslový vzor
  - Požadavek externistů na velké licenční poplatky
  - Pro management nastala obtížně řešitelná situace – hysterická reakce
  - Po návratu k racionálnímu uvažování se situaci podařilo vyřešit
- Jde o problém „kybernetické bezpečnosti“?
- Jde o problém informační bezpečnosti?
- Úplně jiný problém?

A jiný…

- Společnost byla obchodně velmi úspěšná, realizovala výrobek s vysokou přidanou hodnotou a velkou marží
  - Výrobek byl unikátní, obchod byl velmi úspěšný s minimálním úsilím
  - Několik obchodníků založilo své SRO
  - Převedli technickou dokumentaci, zákazníky – prokazatelným způsobem (maily, datová uložiště)
  - Vyráběli jinde, prodávali levněji
  - Společnost se bránila u soudu
  - Soud prohrála – argument soudce – zaměstnanci nevěděli, že jde o obchodní tajemství…

Hořce úsměvné incidenty

- Úniky emailové korespondence politiků
- Nabourání se do účtů na sociálních sítích
- Nabourání se do počítačů
- Extrakce dat
- Ovládnutí technologií

- K čemu stát potřebuje všechna tato data?
  - Podklady pro holokaust…

Uvědomte si

- **Problém informační (kybernetické) bezpečnosti:**
  - Jde o souboj myšlenek – téměř bez technických omezení a limitů
  - **Proaktivní ochrana s účinností 100% je nemožná**
  - Bezpečnostní mechanismy:
    - Pochopení principů
    - Reakce na známá rizika
    - Poučení se ze známých incidentů
    - Předpoklad vývoje
    - Existuje dokonalý antivir?
    - Člověk – nejzranitelnější článek řetězce
  - **Nejnebezpečnější incidenty jsou ty, o kterých se oběť nedozví…**

Shrnutí motivačního úvodu

- **Neexistuje jedna bezpečnost –** vše souvisí se vším
- **S růstem hodnoty rostou rizika**
- **Nepoměr mezi náklady** na útok a jeho možnými dopady
- **Technologie předbíhá bezpečnost**
- **Chybí bezpečnostní zkušenost**
- **„Kyber a informační bezpečnost“ nezná limity ☺**

Nudné základní pojmy

- Základní pojmy:
  - Informace
  - Bezpečnost, informační bezpečnost
  - Kybernetická a informační bezpečnost
  - Přístupy k informační a kybernetické bezpečnosti
  - Informační systém, ICT
  - Digitální stopa
  - Digitální identita

Základní pojmy - informace

- Jak chápete pojmy:
  - Informace
  - Data
  - Informační systém
  - Bezpečnost
  - Kybernetická bezpečnost
  - Informační bezpečnost

Základní pojmy - informace

- **Informace:**
  - Existuje mnoho definic, vybírám:
  - ***Sdělitelný poznatek, který má smysl a snižuje neznalost***
  - Informační šum, fake news…

- **Data:**
  - Vyjádření informací schopné přenosu, uchování, interpretace, zpracování

- Rozdíl data x informace?
- Pojem informace je nutno chápat obecně – ne pouze data v elektronické podobě

- Jednotka informace – 1 bit – víte, co znamená?

Základní pojmy - informace

- Vlastnosti informace důležité pro informační bezpečnost:
  - **Hodnota informace**
  - **Důvěrnost** – souvisí s hodnotou
  - **Dostupnost**
  - **Integrita**
  - Nosič informace - médium:
    - Kamenná deska
    - Lidé
    - IT systémy
    - Papírová dokumentace

    - **Pozor na METADATA**

Specifika informace – hodnota informace

- **Hodnota informace**
  - Hodnota je vlastnost informace
  - Rozdílná hodnota pro jednotlivé subjekty
  - Hodnota informace může být pro vlastníka zanedbatelná, pro útočníka obrovská (veřejná správa)
  - Existují metodiky na oceňování informací:
    - Cenu informace subjekt nejlépe zjistí při incidentu
    - Informace velmi rychle mění hodnotu
  - Vznik rozsáhlých škod:
    - Marketing
    - HOAX
    - Poškození dobrého jména
    - Důvěryhodnost

Specifika informace – informace x hmotná věc

- Rozdílnost podstaty – informace x hmotná věc
  - Ztráta informace x ztráta věci
  - Změna informace x změna věci
  - Podvržená informace x podvržená věc
  - Neúplná informace x neúplná věc
  - Ověření autenticity informace
    - Velmi efektivní nástroje boje – dezinformace

- Rozdíl při identifikaci incidentu – informace x hmotná věc

- **Bezpečnostní incidenty – prolomení bezpečnosti informací – nemusí být nikdy zjištěny**

Specifika informace – informační společnost

- Informační společnost:
  - Informační ekonomika
  - Informace je zbožím, komoditou
  - Informace ovlivňují život každého jedince
  - Informační politika – PR týmy ☹
  - Kde je míra?
    - Jedním z aspektů posouzení míry je bezpečnost
    - Bohužel míra potřeby bezpečnosti se u subjektů liší
    - Liší se i hodnota informace
    - Vyostřující se spor:
      - Míra osobní svobody x informace poskytované státu

Specifika informace – informační společnost

- „Nečekané problémy“:
  - Ověření autenticity dříve x dnes
  - Etické normy – je normální lež premiéra?
  - Dostupnost informací
  - Rychlost šíření informací
  - Změna hodnoty informace
  - Záměna identity
  - Dosažení soukromí a anonymizace
  - Co je informace a co šum

- V technologiích se ztrácí člověk a lidský faktor
- Odpovědní manageři a úředníci nechápou principy
- Ovládnutí komunikace – ovládnutí společnosti?

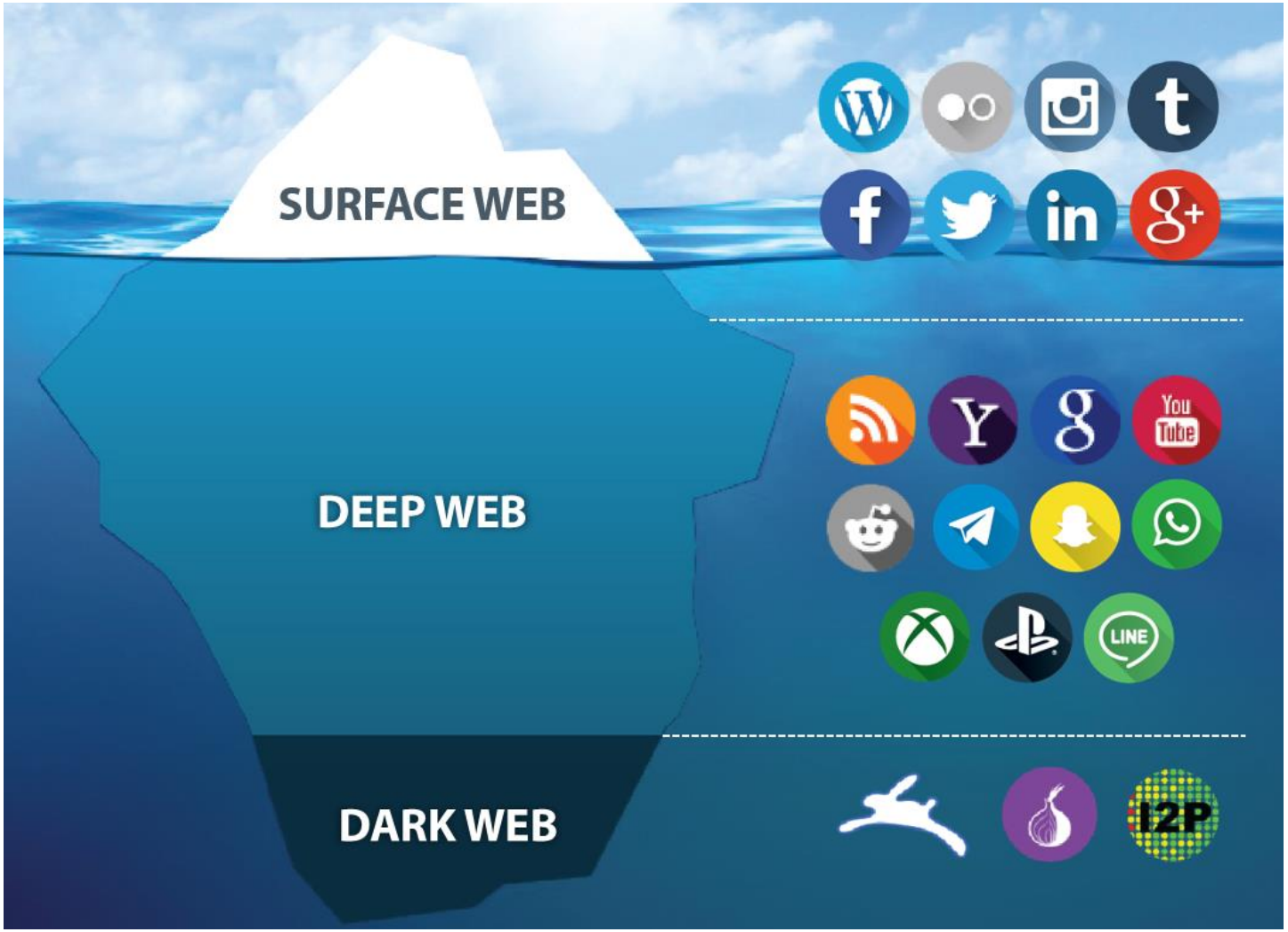
Kybernetický prostor – Cyberspace

- Neexistuje jednotná a ucelená definice
- Definice v zákoně č. 184/2014 o kybernetické bezpečnosti:
  - ***Digitální prostředí umožňující vznik, zpracování a výměnu informací tvořené informačními systémy, službami a sítěmi elektronických komunikací***
    - Nejen globální počítačová síť sítí s probíhající online komunikací
    - Často se chybně zužuje pouze na internet
    - Jde o širší virtuální prostor

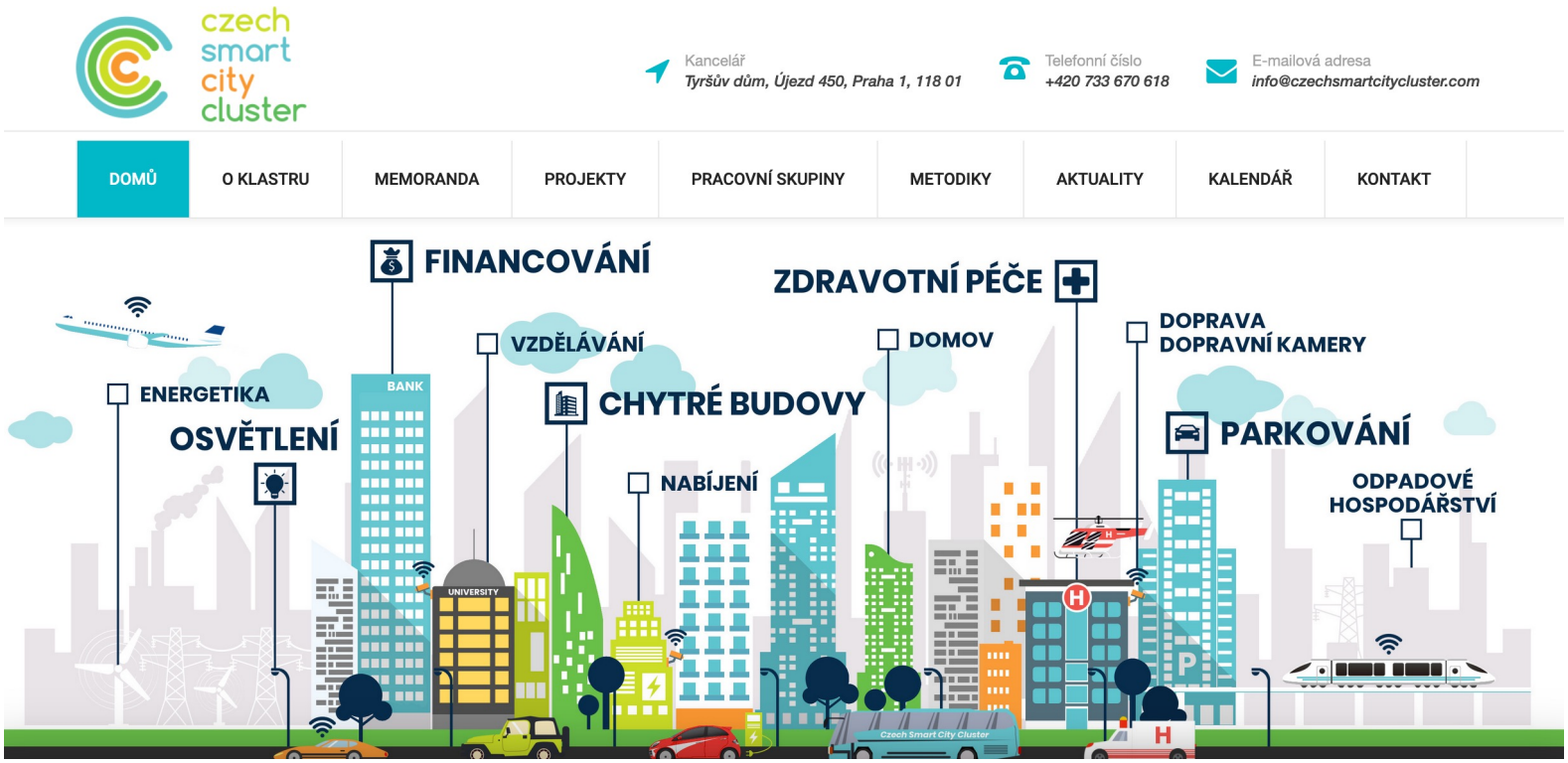
Kybernetický prostor – Cyberspace

- Vlastnosti podstatné pro bezpečnost:
  - Míra otevřenosti systému – otevřený x uzavřený digitální systém
  - Přístupnost širokému okruhu uživatelů – vynutitelnost autentizace uživatele
  - **Pocit** anonymity – velikost zdrojů na identifikaci
  - Obtížnost vynutitelné regulace v globálním měřítku
    - Což může být výhodou ☺
    - Míra regulace x svoboda
  - **Vytěžování dat a metadat**
- Pochopitelnost principů pro běžné uživatele
- Vytváření bezpečnostních návyků a chování

Kyber prostor – co zahrnuje

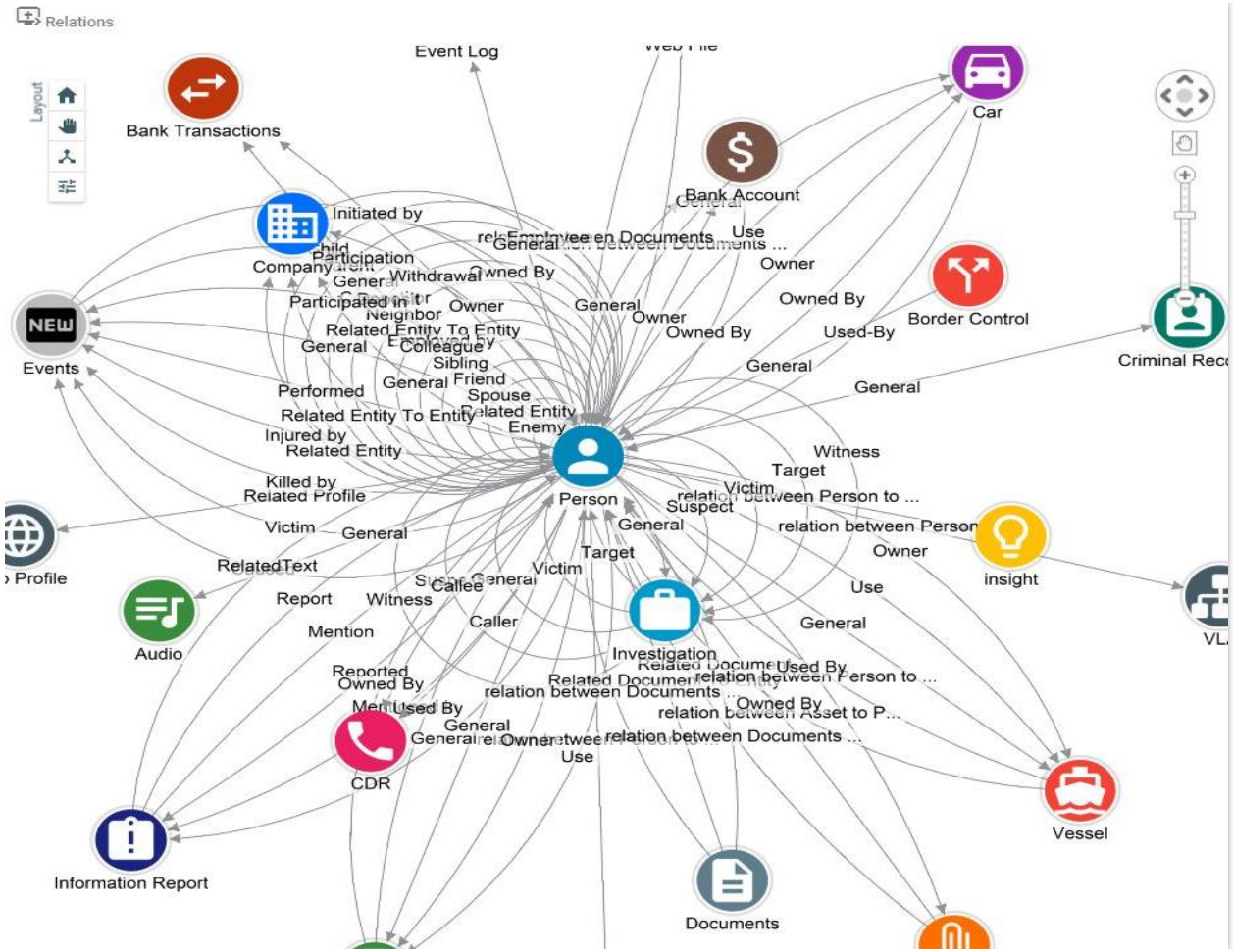


Kyber prostor – chytrá města, IoT



https://czechsmartcitycluster.com/

Interakce s kyber prostorem



https://www.verint.com/

VIAVIS střežíme podstatné

Některé vlastnosti kyber prostoru

- Neexistence anonymity
- Digitální stopa
- Svět víry
- Metadata
- Retrospektiva
- Limity

Svět víry

									
Flashlight Apps	Super-Bright LED Flashlight	Brightest Flashlight Free	Tiny Flashlight + LED	Flashlight	Flashlight	Brightest LED Flashlight	Color Flashlight	High-Powered Flashlight	Flashlight HD LED
Permissions									
retrieve running apps	✓					✓		✓	
modify or delete the contents of your USB storage	✓	✓				✓		✓	
test access to protected storage	✓	✓				✓		✓	
take pictures and videos	✓	✓	✓	✓	✓	✓	✓	✓	✓
view Wi-Fi connections	✓	✓				✓		✓	✓
read phone status and identity	✓	✓			✓	✓		✓	
receive data from Internet	✓					✓		✓	
control flashlight	✓	✓	✓			✓	✓	✓	✓
change system display settings	✓					✓		✓	
modify system settings	✓					✓		✓	
prevent device from sleeping	✓							✓	
view network connections	✓	✓	✓	✓	✓	✓	✓	✓	✓
full network access	✓	✓	✓	✓	✓	✓	✓	✓	✓
approximate location (network-based)	✓	✓						✓	
precise location (GPS and network-based)	✓	✓						✓	
disable or modify status bar	✓	✓							
read Home settings and shortcuts	✓	✓		✓					
install shortcuts	✓	✓		✓					
uninstall shortcuts	✓	✓		✓					
control vibration	✓		✓						
prevent device from sleeping		✓	✓	✓		✓			✓
write Home settings and shortcuts				✓					
disable your screen lock				✓					
read Google service configuration					✓				✓

Co ví telekomunikační operátor – ne anonymita

https://www.usetreno.cz/telco-score/

Telco Scoring – ne anonymita

Dobrý den, Aleši. TelcoScore využíváme. Je dobrý pro klienty, kteří nemají úvěrovou historii. Váha je interním kritériem. Odmítnou se nedá. Hezký den. Jitka, Equa bank

— Equa bank (@equabankcz) 16. prosince 2017

Dobrý den, Aleši, posíláme slíbené bližší informace: V tuto chvíli používáme TelcoScore v pilotním režimu. Předpokládáme, že díky tomuto nástroji budeme schopni poskytnout půjčky většímu procentu zejména mladých lidí, kteří nemají dostatečnou bankovní historii.

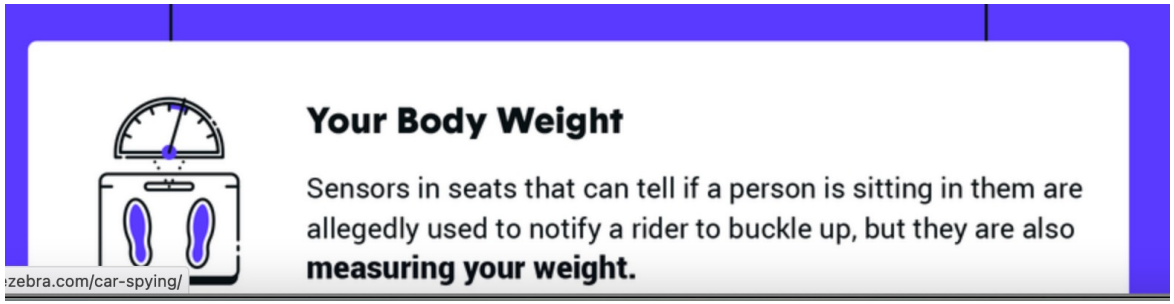
— Česká spořitelna (@Ceskasporitelna) 16. prosince 2017

https://www.e15.cz/finexpert/pujcujeme-si/velky-bratr-vas-sleduje-24-7-banky-si-klienty-mohou-proklepnout-dle-telcoscore-1341152

Co monitorují automobilky – ne anonymita

https://www.skoda-auto.cz/modely/karoq/karoq-sportline/karoq-sportline-konektivita

Co monitorují automobilky – ne anonymita



https://hakin9.org/what-data-does-your-car-collect-on-you-infographic-by-the-zebra/

Retrospektivní rizika

Zpravodajství Sport iVysílání TV program Pořady A–Z Pro děti Art edu Vše o ČT

ČT24

KORONAVIRUS AMERICKÉ VOLBY KRAJSKÉ VOLBY DOMÁCÍ SVĚT REGIONY EKONOMIKA

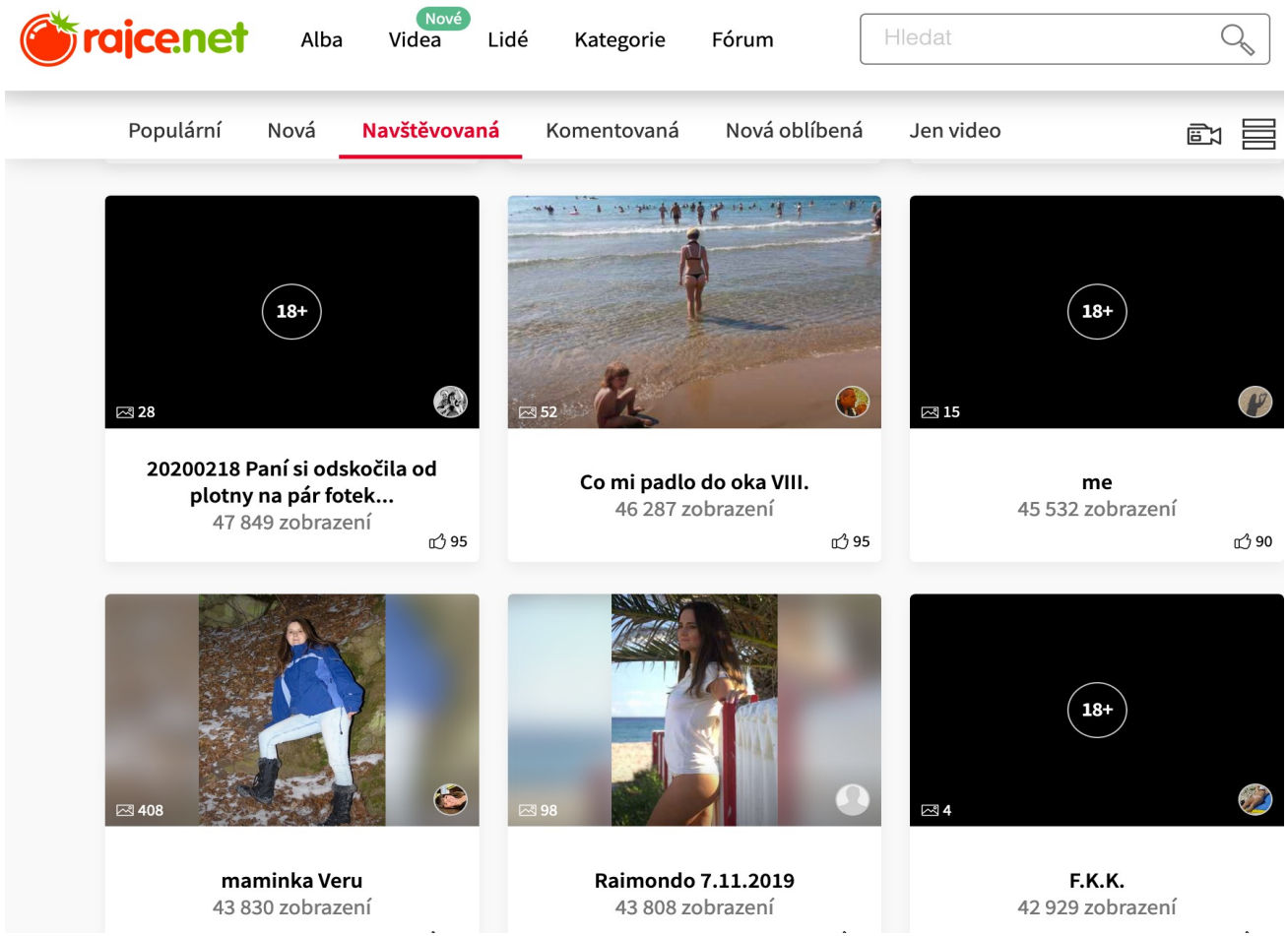
Kanadou otřásla fotka premiéra převlečeného za černocha. Trudeau se omlouvá, opozice je v šoku

19. 9. 2019

Kampaň kanadského premiéra Justina Trudeaua před říjnovými volbami poznamenalo zveřejnění 18 let staré fotografie, na níž má černý obličej a turban. Politik se omlouvá za rasismus, opoziční konzervativci mluví o šoku a zklamání. Černobílý snímek, který zveřejnil časopis Time, vznikl na karnevalu ve škole, kde Trudeau učil.

VIAVIS střežíme podstatné

Digitální stopy - retrospektiva



I toto je kyber svět a kyber bezpečnost

Economy / China Economy

Explainer | What is China's social credit system and why is it controversial?

- China's social credit system is a set of databases and initiatives that monitor and assess the trustworthiness of individuals, companies and government entities
- A good rating could offer priority health care or deposit-free renting of public housing, while a negative rating could see individuals banned from flights and trains

Amanda Lee in Beijing
Published: 12:00pm, 9 Aug, 2020

Why you can trust SCMP

https://www.scmp.com/economy/china-economy/article/3096090/what-chinas-social-credit-system-and-why-it-controversial

Základní pojmy – bezpečnost

- **Bezpečnost není stav** – častý omyl (nic není absolutně bezpečné)
- **Je vlastnost aktiva určená svou mírou – schopností odolávat hrozbám**

- Neexistuje „oddělená bezpečnost“
  - BOZP
  - Informační
  - Kybernetická
  - Fyzická
  - Personální
  - Krizová
  - Administrativní
  - Procesní
  - …

Základní pojmy – bezpečnost informace

- **Bezpečnost = zajištění důvěrnosti, dostupnosti a integrity informace**

  ISO/IEC 27001

  - **Důvěrnost** – zajištění přístupu k informacím pouze oprávněným osobám
  - **Dostupnost** – zajištění přístupu k informacím v požadovaném čase
  - **Integrita** – zajištění celistvosti a neměnnosti informace:
    - Zobrazená data jsou totožná se zdrojovými
    - Data jsou kompletní, nic nechybí
    - Neexistují osiřelá data (SPZ bez auta…)
    - Zachování dat v jejich definované struktuře
    - Zabezpečení dat u prováděných změn:
      - Odolnost proti neoprávněným změnám
      - Identifikace pokusů o neoprávněnou změnu

Základní pojmy – bezpečnost informace

- **Bezpečnost - ochrana informací:**
  - Během jejich **vzniku, zpracování, ukládání, přenosu a likvidace**
  - Využitím **logických, technických, fyzických a organizačních opatření**
  - Všechny aspekty musí být v souladu:
    - Technická bezpečnost x chování uživatele
    - Bezpečnost x komfort užívání
    - Nesoulad generuje hrozby

Základní pojmy – bezpečnost systému

- Bezpečnost není jen funkcí systémů zpracovávajících informace
- Bezpečnost systému není pouze funkcí bezpečnosti jednotlivých komponent
- Bezpečný celek není pouhé sestavení z bezpečných prvků

- **Požadavky na bezpečnost systému:**
  - Systém jehož činnost nezpůsobuje nebezpečné stavy
  - Každá porucha vede bezpečným směrem
  - Míra bezpečnosti x míra spolehlivosti
  - Bezpečnostní incidenty lze identifikovat
  - Je definována míra bezpečnosti

Kybernetický prostor – bezpečnost

- **Komplexní zajištění bezpečnosti:**
  - Informací
  - Systémů
  - Uživatelů
  - Poskytovaných služeb
  - Na výše uvedeném závislých aktiv:
    - Businessu
    - Ekonomiky
    - Organizací
    - Státu
    - Jednotlivců
    - …..

VIAVIS střežíme podstatné

Základní pojmy – bezpečnostní incident

- **Bezpečnostní incident** – prolomení důvěrnosti, dostupnosti nebo integrity

- Aspekty bezpečnostních incidentů:
  - Identifikace
  - Klasifikace
  - Reakce - protiopatření
  - Měření účinnosti protiopatření
  - Časové hledisko
  - Dopad incidentu
  - Poučení – nápravná opatření

Kyber kriminalita

- Úmyslné bezpečnostní incidenty v kyberprostoru
- Nelze je zužovat pouze na několik málo medializovaných typů

- Cíle:
  - Zisk pro útočníka
  - Poškození protivníka
  - Politické cíle
  - Něco si dokázat
  - Zjištění informací
  - Manipulace, vydírání
  - Získání zdrojů
  - Získání kontroly nad obětí
  - Útočníka to „pouze“ baví

  - **Opakování – nejhorší dopady mají incidenty, o nichž se oběť nedozví**

Několik užitečných pouček

- **Míra bezpečnosti je daná mírou ochrany nejslabšího článku vůči hrozbě**

- Neplatí extrémy:
  - Absolutní ochrana – ochrana proti všem myslitelným rizikům
  - Žádná ochrana – nemá smysl informace chránit, stejně vždy uniknou

- Prevence je vždy levnější, než náklady na řešení incidentu a vzniklé škody
  - Pokud je vůbec možná

- Bezpečnostní aspekty je třeba zahrnout již do návrhu systému
  - Ex post implementace je vždy nákladnější
  - Paradox – lze vůbec implementovat proaktivní bezpečnost?

Přístupy k informační bezpečnosti

- Nutno si uvědomit – bezpečnost je jen jedna a její míra je dána mírou nejslabšího článku
- Přístup k informační bezpečnosti dle způsobu řešení:
  - Informační bezpečnost není řešena
  - Ad hoc přístup
  - „Default“ přístup
  - Hysterický přístup
  - Základní přístup
  - Přístup na základě managementu rizik – zvládání rizik
  - Integrovaný systematický přístup založený na relaci s hodnotou aktiv
  - *Přemýšlejte – kdy má který přístup smysl?*

  - *Co může udělat stát?*

Přístupy k informační bezpečnosti

- Přístup k informační bezpečnosti dle oblastí:
  - IT bezpečnost
  - Personální bezpečnost
  - Objektová bezpečnost
  - Fyzická bezpečnost
  - Přesah do BOZP, QMS, EMS, FMEA
  - *Přemýšlejte – kdy má který přístup smysl?*

  - ***Na jaký argument slyší manažeři a politici? ☺***

Systematické řešení informační bezpečnosti

- Základní požadavky:
  - Pokrytí všech oblastí, kde se aktiva vyskytují
  - Ochranná opatření musí být integrovaná (teorie nejslabšího článku)
  - Náklady na ochranu musí být v relaci s hodnotou aktiv

- Efektivní přístup:
  - Systematický a integrovaný systém řízení managementu informační bezpečnosti založený na managementu - zvládání rizik
  - Best practices – technické normy a standardy

… více v samostatné přednášce

Informační systém

- **Systém, který zpracovává informace**
  - Jakýkoli systém – nejen IT (kartotéka, telekomunikační systémy…)

- Co to je zpracování:
  - Získání informací – transformace na data
  - Uchování, zpracování, propojení, přenos dat
  - Interpretace dat – transformace na informaci
  - Z mnoha informací poskytnout interpretaci těch nejdůležitějších
  - Zničení nepotřebných dat
  - Vznik metadat

Informační a komunikační technologie – IT, ICT

- Technologie pro pořizování, získávání, zpracování, přenos, uchování, ničení a vyhledávání informací

- Historicky se oddělovaly IT a komunikační technologie
- Dnes toto oddělení postrádá smysl

- ICT proniká do nových oblastí:
  - Provoz domácností
  - Zábava
  - Automotive
  - Veřejný prostor
  - Soukromý život

Informační systém

- Jakákoli **systematická** práce (zpracování) s informacemi
- Lze jej modelovat různě:
  - HW, SW, datové přenosy, procesy, lidé, metody
  - Automatizované systémy
  - Neautomatizované systémy (telefonní seznam)
- Pro ochranu informací je nutné postihnout úplný systém (vše, kde se informace vyskytují)
- Přemýšlejte, lze chránit informace u nesystematické práce s nimi?
- Lze chránit veškeré informace?

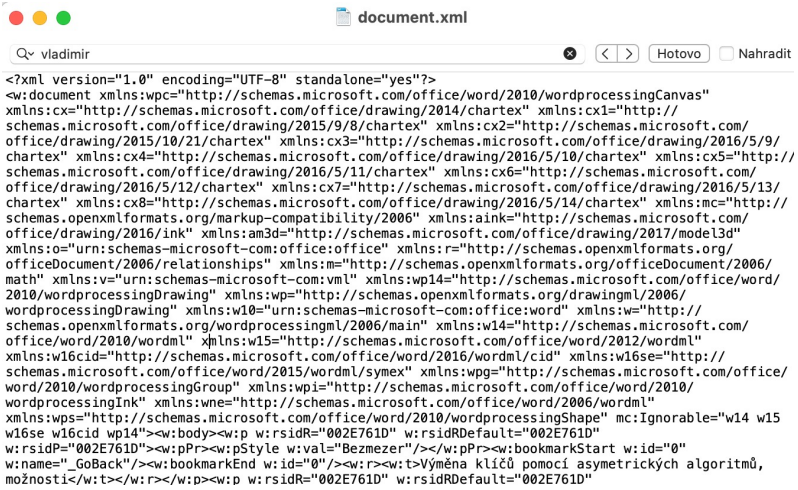
Digitální stopa

- Jakákoli **interakce** s kyber prostorem
- Vzniká na různých úrovních
- **Uživatel ji nikdy nemá zcela pod kontrolou**
- **Nelze se jí zbavit**

- Lze ji pouze částečně zastřít

- Metadata = data o datech

Metadata – ukázka .docx -> .zip



VIAVIS střežíme podstatné

Metadata - ukázka

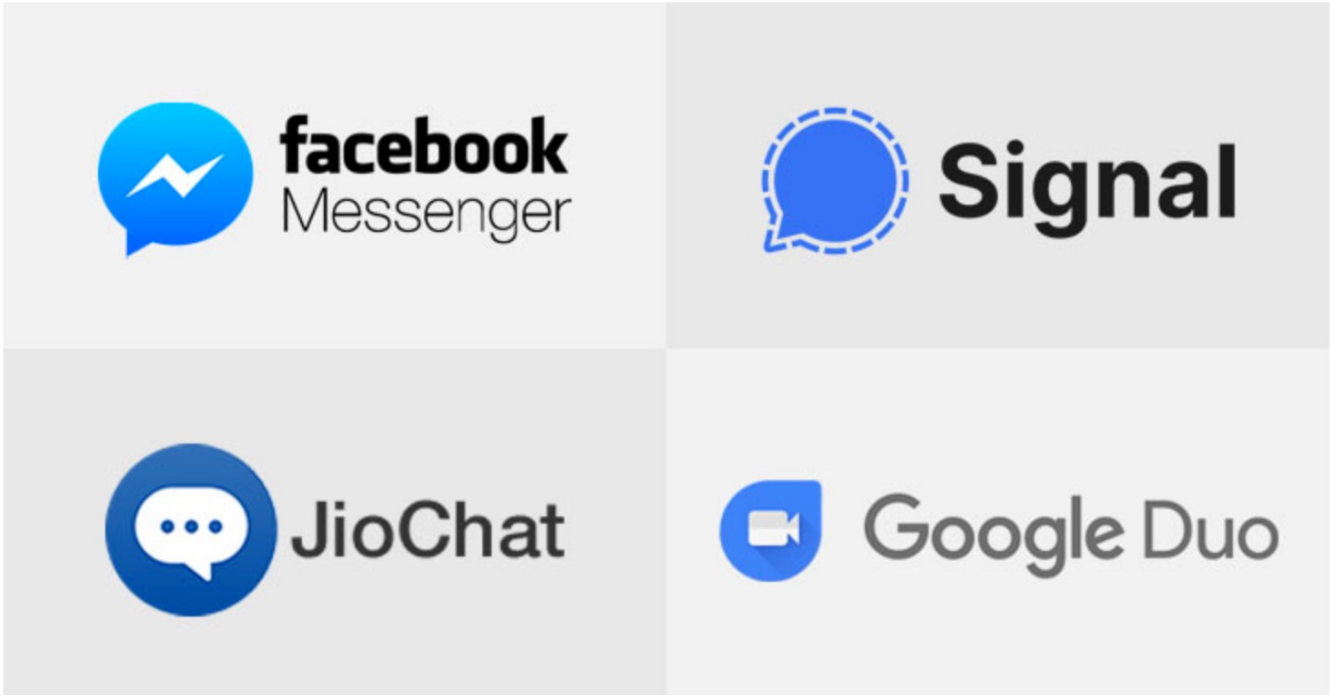
- Nejedná se pouze o office dokumenty
- https://support.microsoft.com/cs-cz/office/odebr%C3%A1n%C3%AD-skryt%C3%BDch-dat-a-osobn%C3%ADch-%C3%BAdaj%C5%AF-kontrolou-dokument%C5%AF-prezentac%C3%AD-nebo-se%C5%A1it%C5%AF-356b7b5d-77af-44fe-a07f-9aa4d085966f

- Mnoho návodů nejen na youtube:
  - https://www.youtube.com/watch?v=jsTLn_sbMUc
  - https://www.youtube.com/watch?v=V1mdx4W35UE
  - https://support.microsoft.com/cs-cz/office/video-odebr%C3%A1n%C3%AD-osobn%C3%ADch-dat-ze-soubor%C5%AF-17b30a75-206f-44e0-9de3-afeedbf6bfa1

- **Co je v kyber prostoru nelze vzít zpět…**

Google Details Patched Bugs in Signal, FB Messenger,

January 20, 2021 Ravie Lakshmanan



https://thehackernews.com/2021/01/google-discloses-flaws-in-signal-fb.html

Odezvy výrobců – všimněte si dat odstranění…

- **Signal** (fixed in September 2019) - A audio call flaw in Signal's Android app made it possible for the caller to hear the callee's surroundings due to the fact that the app didn't check if the device receiving the connect message from the callee was the caller device.

- **JioChat** (fixed in July 2020) and **Mocha** (fixed in August 2020) - Adding candidates to the offers created by Reliance JioChat and Viettel's Mocha Android apps that allowed a caller to force the target device to send audio (and video) without a user's consent. The flaws stemmed from the fact that the peer-to-peer connection had been set up even before the callee answered the call, thus increasing the "remote attack surface of WebRTC."

- **Facebook Messenger** (fixed in November 2020) - A vulnerability that could have granted an attacker who is logged into the app to simultaneously initiate a call and send a specially crafted message to a target who is signed in to both the app as well as another Messenger client such as the web browser, and begin receiving audio from the callee device.

- **Google Duo** (fixed in December 2020) - A race condition between disabling the video and setting up the connection that, in some situations, could cause the callee to leak video packets from unanswered calls.

https://thehackernews.com/2021/01/google-discloses-flaws-in-signal-fb.html

Digitální stopa a anonymita

Anonymity and privacy are not about closing the door when you go to the bathroom. For the individual, they might be about personal autonomy, political liberty or just protecting yourself in the digital world.

https://www.csoonline.com/article/2975193/9-steps-completely-anonymous-online.html

VIAVIS střežíme podstatné

Jaké záznamy na internetu vznikají – digitální stopy

- Data uložená uživateli
- Obsah komunikace
- Záznamy o aktivitách

https://www.techrepublic.com/article/encrypting-communication-how-and-why-to-do-it-well/

Kdo má k digitální stopě přístup

ODPOSLECHY

Úvodní strana / O nás / Bezpečnostní politika / Odposlechy

Analýzy odposlechů a záznamů telekomunikačního provozu a sledování osob a věcí dle trestního řádu a rušení provozu elektronických komunikací Policií ČR - archiv

Rok 2019 (pdf, 7,5 MB)

Policie ČR

Hasiči ČR

https://www.mvcr.cz/clanek/analyzy-odposlechu-a-zaznamu-telekomunikacniho-provozu-a-sledovani-osob-a-veci-dle-trestniho-radu-a-ruseni-provozu-elektronickych-komunikaci-policii-cr-archiv.aspx

Kdo má přístup k digitální stopě

- Zákon o telekomunikačních službách
- Kdokoli, kdo má přístup ke komunikaci
- Kdokoli, kdo má přístup k obsahu
- Provozovatelé služeb
- Útočník s využitím invazivních a neinvazivních metod (OSINT)

Jak chránit své soukromí a být anonymní

- Nejde o triviální problém
- Absolutní anonymity nelze dosáhnout
- Neexistuje jedno všeobjímající řešení
- Řešení:
  - Chování uživatele
  - Kombinace technických opatření
  - Bezpečnost je vždy na úkor komfortu

Digitální identita

- Definice
- Konzervativní identita
- Biometriky
- Behaviorální biometriky
- Bezpečnostní pohled

Digitální identita

- Jednoznačná identifikace subjektu v kyber prostoru
    - Osobní identita = jméno, příjmení, další data
    - Zástupná = nickname, email…
    - Vysoká míra záruky, že subjekt je tím, za koho se vydává

Digitální identita

Co je digitální identita?

Digitální identita představuje elektronický prostředek pro identifikaci osob. Tvoří ji certifikát obsahující „veřejný klíč“, který lze zobrazit, a „soukromý klíč“, který je soukromý.

https://support.apple.com/cs-cz/guide/mac-help/mchlp2695/mac

Zákonné úpravy digitální identity

Portál národního bodu pro identifikaci a autentizaci

Národní bod slouží jako nástroj pro bezpečné a zaručené ověření totožnosti uživatele online služeb veřejné správy. Poskytovatelé online služeb potřebují zaručenou informaci o tom, kdo se jako klient přihlašuje k jimi poskytovaným službám.

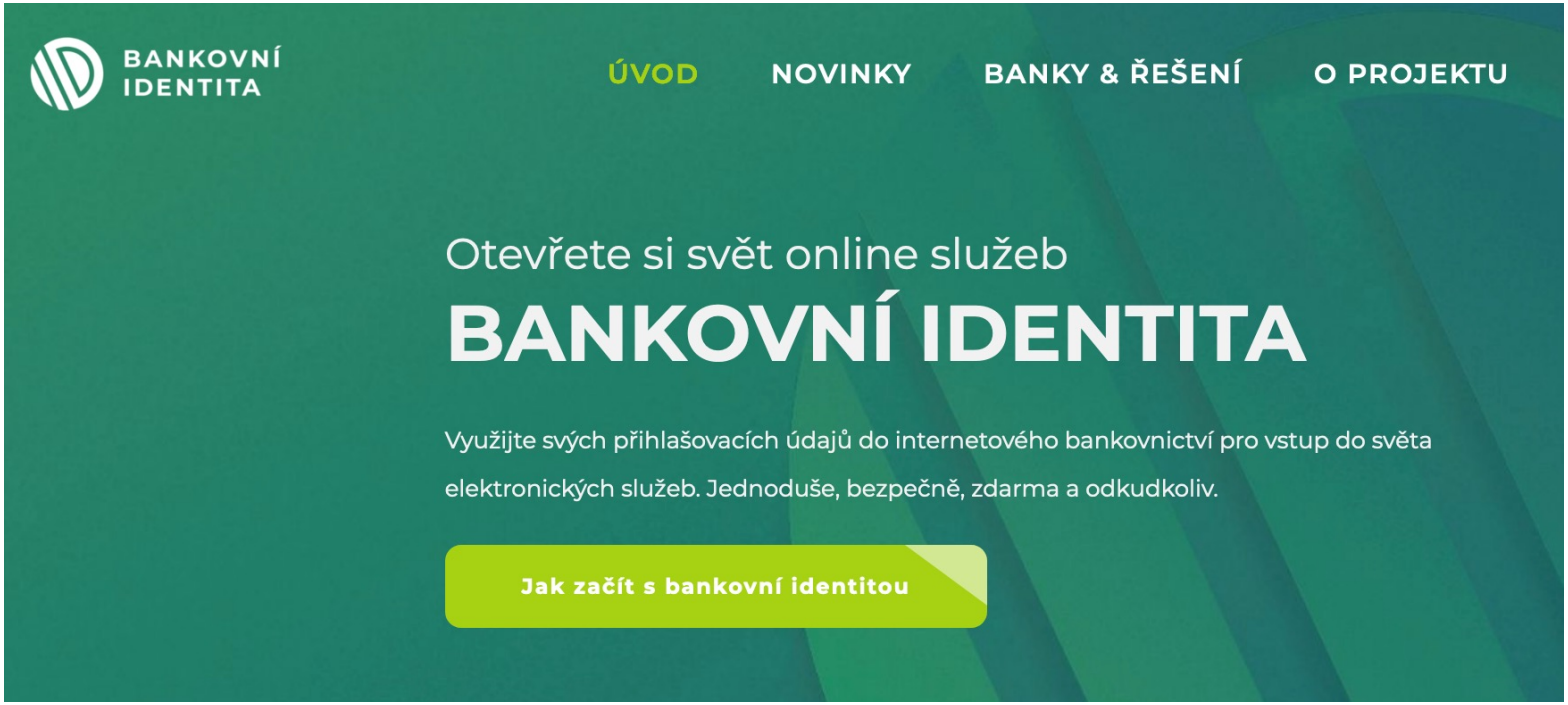
K prokazování totožnosti online slouží různé identifikační prostředky, jejichž poskytovatelé získali akreditaci a jsou napojeni na národní bod. Mezi ně patří například nový občanský průkaz s čipem, který je vydáván od 1. 7. 2018, nebo přihlášení pomocí uživatelského účtu národní identitní autority.

Veškeré údaje jsou poskytovatelům služeb předávány pouze v případě, že k tomu v procesu přihlašování udělíte souhlas.

Národní bod je zřízen zákonem č. 250/2017 Sb., o elektronické identifikaci, který zároveň stanovuje pravidla pro účastníky procesu elektronické identifikace.

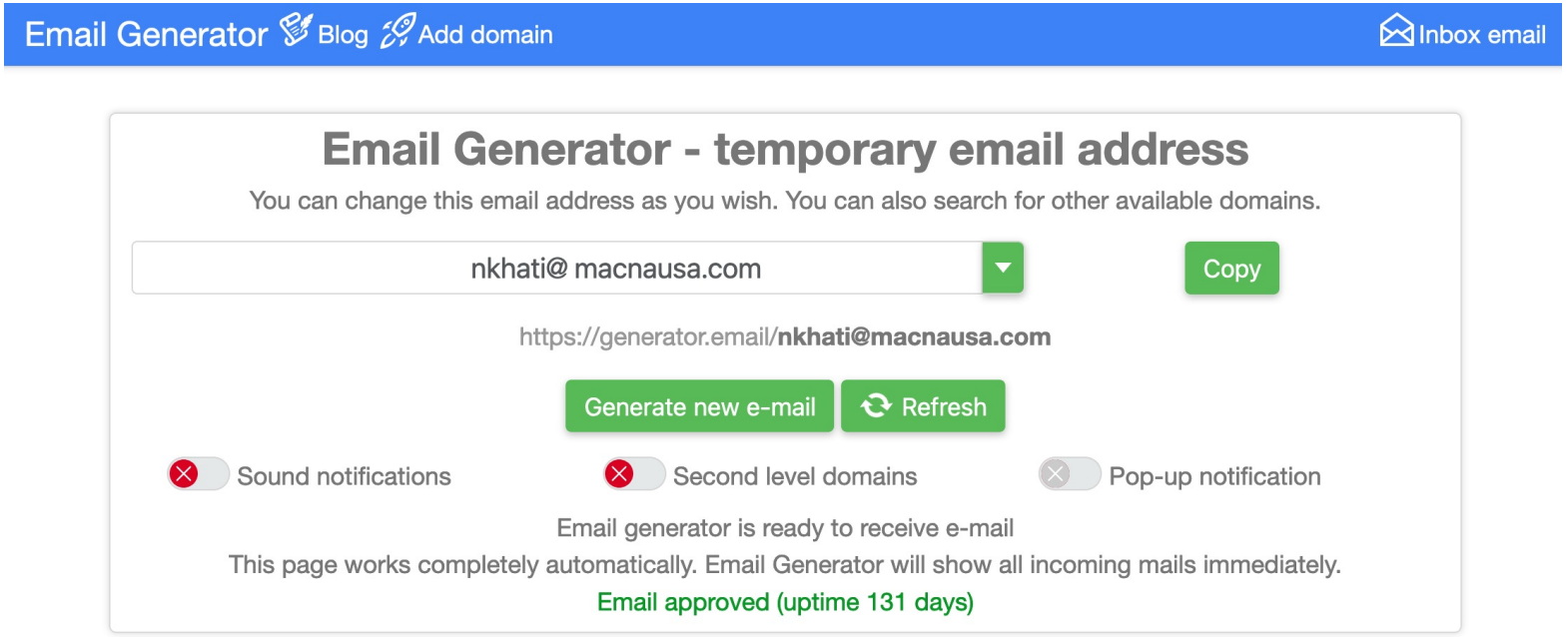
https://www.eidentita.cz/Home

Projekt bankovní identity



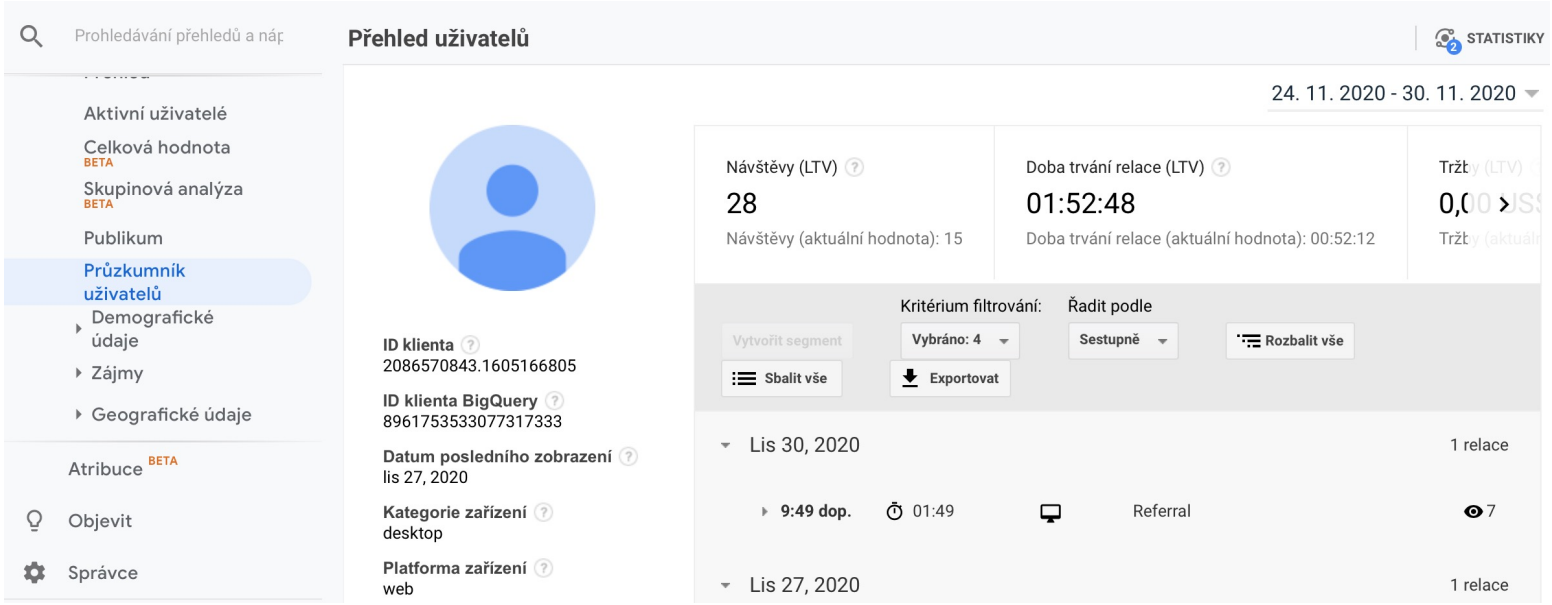
https://bankovni-identita.cz/

Proč je digitální identita důležitá



https://generator.email/

Pro koho je digitální identita důležitá



https://analytics.google.com/analytics/web/...

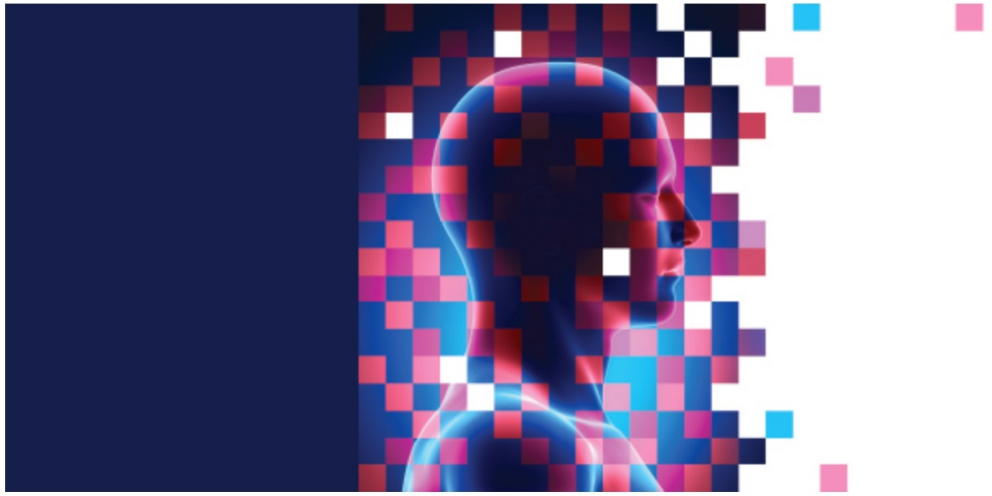
VIAVIS střežíme podstatné

Motivace útoků na identitu

COMPLIANCE, SEPTEMBER – NOVEMBER 2019, SPECIAL FOR THE WEB

Digital Identity and Financial Crimes

SEPTEMBER 4, 2019



https://www.acamstoday.org/digital-identity-and-financial-crimes-2/

VIAVIS střežíme podstatné

Konzervativní digitální identita

– Je poskytována dobrovolně

– Využívá mechanismů s vědomím a kontrolou uživatele

– https://www.seznam.cz/

Back to basics: Multi-factor authentication (MFA)

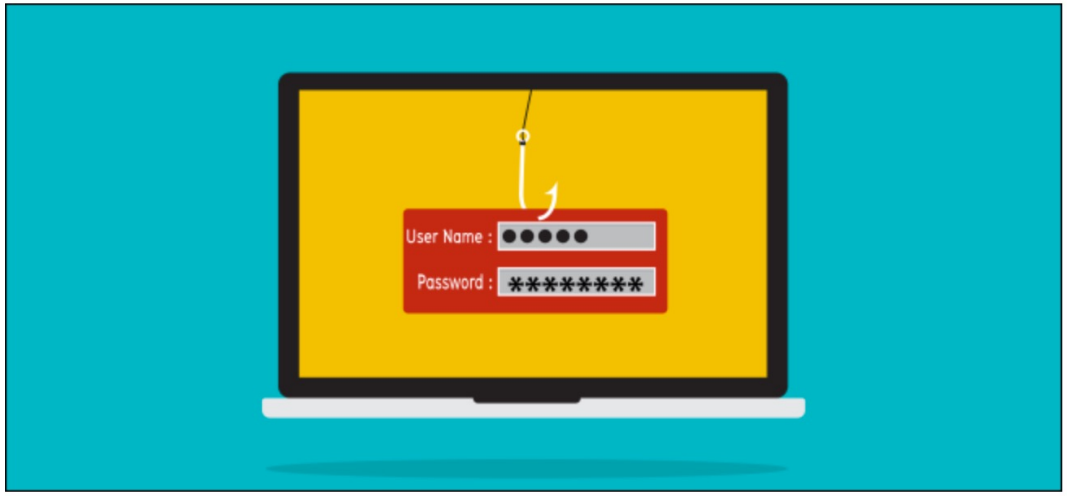
Here's the traditional, not so secure way to log in to your bank account: enter your username and that familiar password you probably use for most of your online accounts. Then, you're in. You can go about your business.

https://www.nist.gov/itl/applied-cybersecurity/tig/back-basics-multi-factor-authentication

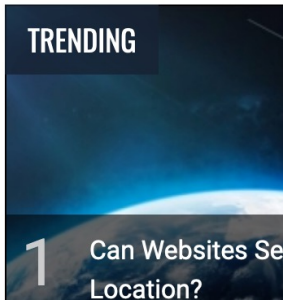
Hesla, hesla, hesla

How to Check if Your Password Has Been Stolen

CHRIS HOFFMAN @chrisbhoffman
UPDATED JULY 10, 2020, 1:11PM EDT



Many websites have leaked passwords. Attackers can download databases of usernames and passwords and use them to "hack" your accounts. This is why you shouldn't reuse passwords for important websites, because a leak by one site can give attackers everything they need to sign into other accounts.



https://www.howtogeek.com/343947/how-to-check-if-your-password-has-been-stolen/

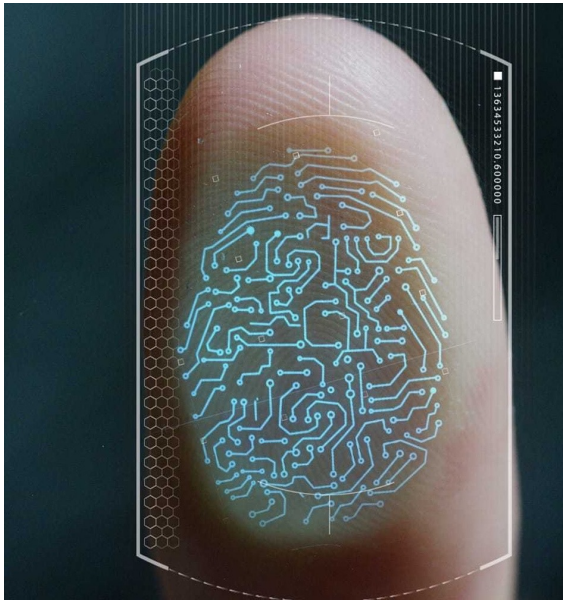
Několik doporučení

- **Svou identitu je třeba chránit**
  - Vědět kde a jakou jsme poskytli
  - Rozdělení identit
  - Ověřovat hesla
  - Vysoké požadavky na bezpečnost:
    - Hesla v hlavě
    - Více faktové ověření

Biometriky a digitální identita

– Proč se využívají stále častěji?

– Největší slabina biometrik?

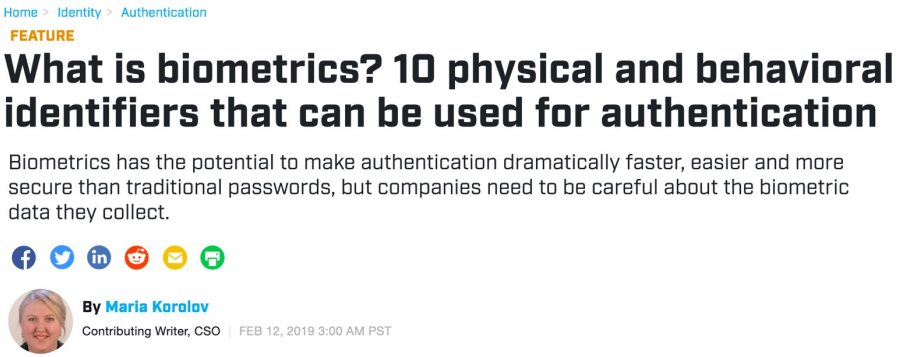


VIAVIS střežíme podstatné

Biometriky

– Fyzické biometriky:

  – Otisky prstů
  – Obličej
  – Oční rohovka, oční duhovka
  – Tvar uší
  – Krevní řečiště v dlani
  – Hlas
  – Digitální podpis
  – DNA



Home > Identity > Authentication

FEATURE

What is biometrics? 10 physical and behavioral identifiers that can be used for authentication

Biometrics has the potential to make authentication dramatically faster, easier and more secure than traditional passwords, but companies need to be careful about the biometric data they collect.

By Maria Korolov
Contributing Writer, CSO | FEB 12, 2019 3:00 AM PST

https://www.csoonline.com/article/3339565/what-is-biometrics-and-why-collecting-biometric-data-is-risky.html

Biometriky

https://duo.com/labs/research/the-good-and-bad-of-biometrics

Nekonzervativní digitální identita

- Nemáme ji tak úplně pod kontrolou
- Založená na Big Data
- Využívá umělou inteligenci
- Vzniká i u poskytovatele služby
- Biometrika založená na analýze chování

May 13, 2019, 09:00am EDT

Behavioral Biometrics Is The Future Of User Authentication

Todd Rebner Forbes Councils Member
Forbes Technology Council COUNCIL POST | Paid Program
Innovation

POST WRITTEN BY
Todd Rebner

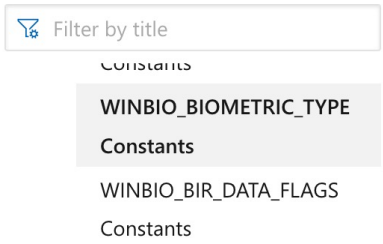
Chief Technology Officer of Cyleron, an artificial intelligence enabled cybersecurity software and solutions company.

https://www.forbes.com/sites/forbestechcouncil/2019/05/13/behavioral-biometrics-is-the-future-of-user-authentication/

Behaviorální biometriky – co využívají

- Způsob psaní na klávesnici
- Pohybové charakteristiky
- Používání myši nebo touchpadu
- Chování v kyber prostoru:
  - Interakce s technologií
  - Využívání aplikací
  - Režim vybíjení baterií
  - Lokace užívání, geolokace
  - Využívání soc. sítí
  - Vztahy
  - Zájmy a interakce na zprávy

Behaviorální biometriky – některé implementace



WINBIO_TYPE_KEYSTROKE_DYNAMICS	The speed and error patterns in typing by an individual are used to determine the identity of an individual.
WINBIO_TYPE_LIP_MOVEMENT	The changes in the lips of an individual that occur when they speak are used to determine the identity of an individual.

https://docs.microsoft.com/en-us/windows/win32/secbiomet/winbio-biometric-type-constants

Behaviorální biometriky – některé implementace

Apple patent filing details new biometric authentication sensors for wearable devices

Designed to understand voice commands and silent gestures

Nov 30, 2020 | Alessandro Mascellino

CATEGORIES Biometric R&D | Biometrics News | Wearable Technology

https://www.biometricupdate.com/202011/apple-patent-filing-details-new-biometric-authentication-sensors-for-wearable-devices

Behaviorální biometriky – Google Android

Google to offer Android login based on behavioral biometrics by end of year

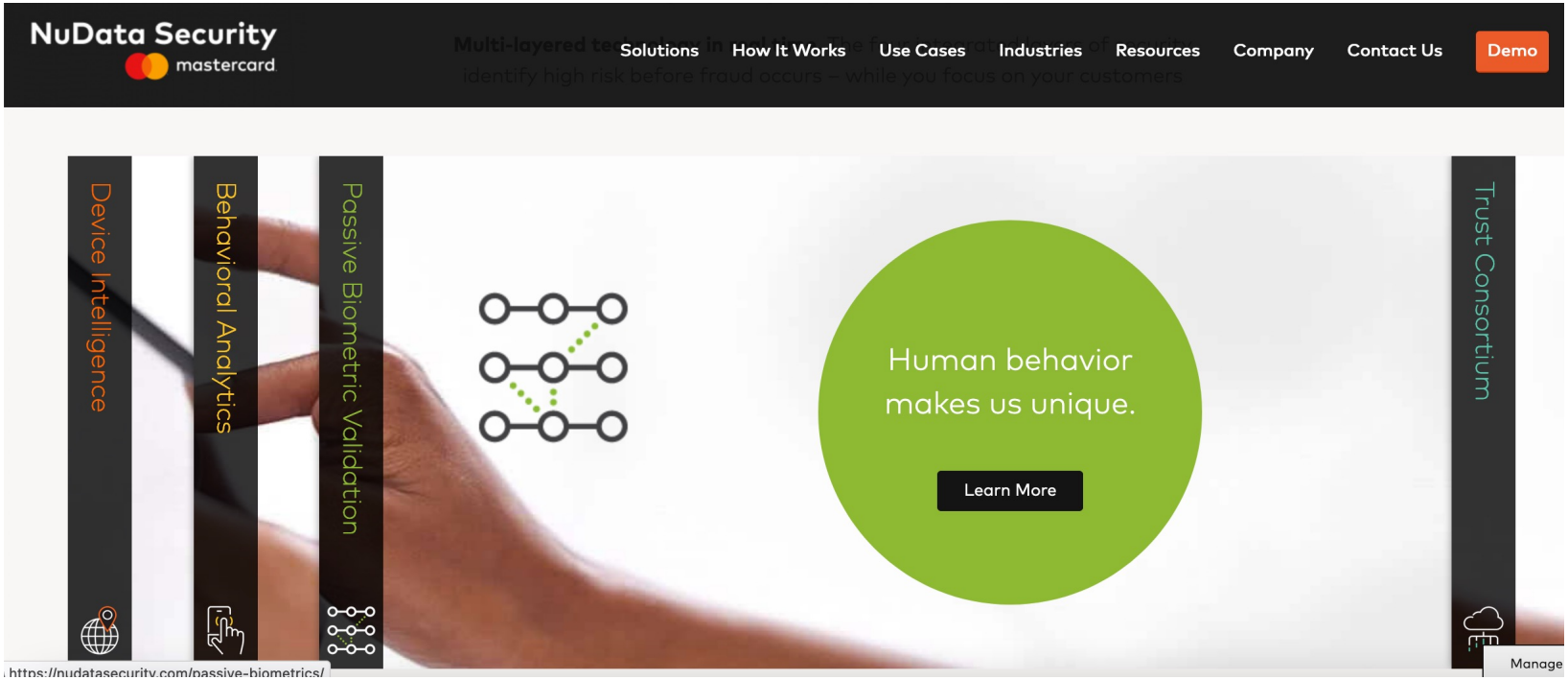
May 24, 2016 | Justin Lee

CATEGORIES Access Control | Behavioral Biometrics | Biometrics News

Google will begin trialing "several large financial institutions" next month in preparation for the upcoming launch of Project Abacus, which aims to make Android apps password free by the end of the year, according to a report by International Business Times.

https://www.biometricupdate.com/201605/google-to-offer-android-login-based-on-behavioral-biometrics-by-end-of-year

Využití v bankovním sektoru

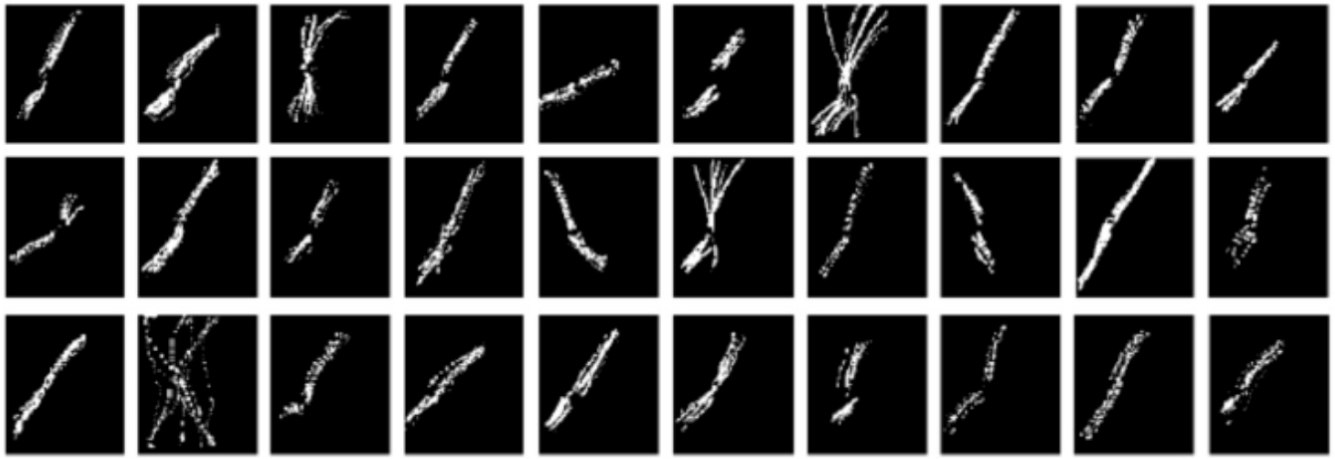


https://nudatasecurity.com/

Mobilní technologie a behaviorální biometriky

Figure 6- available via license: Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International

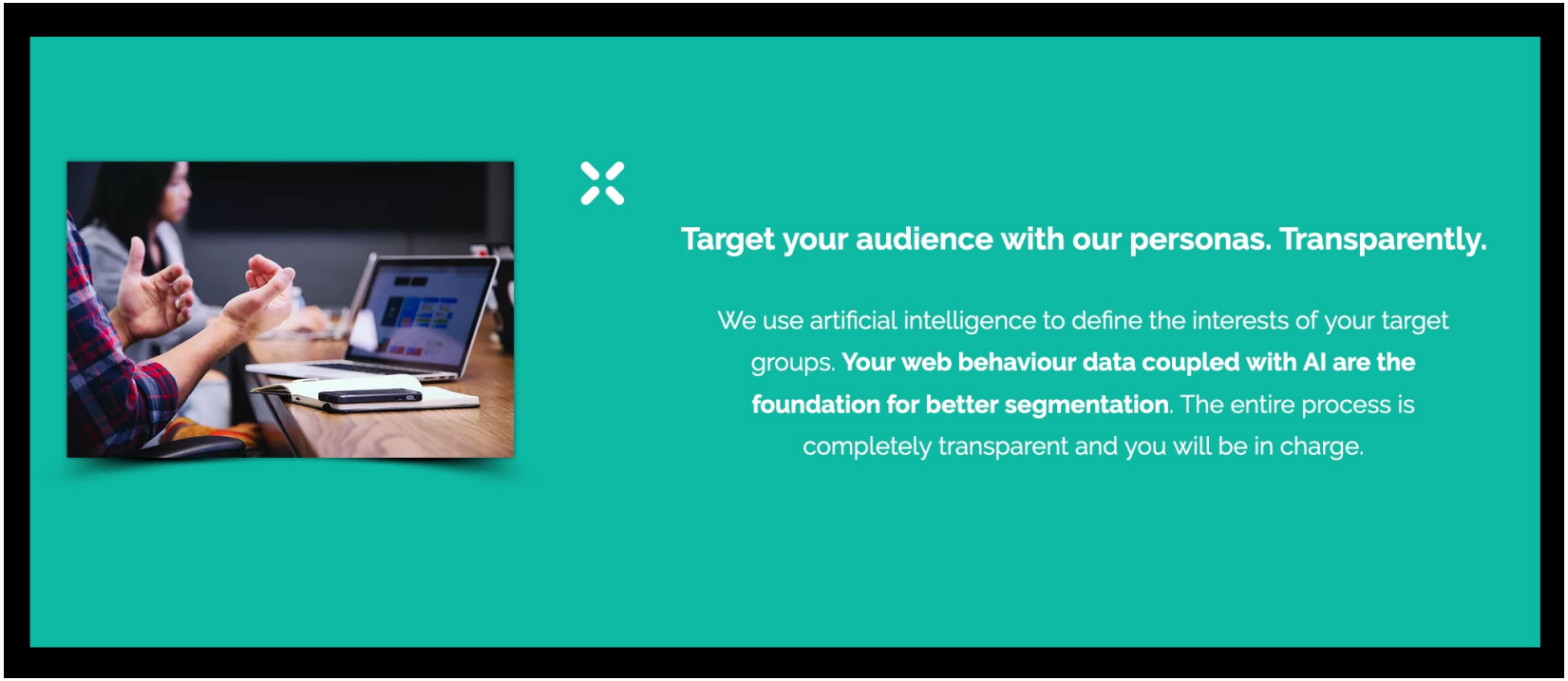
Download View publication



Over 300 touch traces of zoom-in gestures from 30 users. From [68], With permission.

https://www.researchgate.net/figure/Over-300-touch-traces-of-zoom-in-gestures-from-30-users-From-68-With-permission_fig2_337183791

Behaviorální biometriky - využití v reklamě



https://www.adpicker.ai/

Behaviorální biometriky shrnutí

- Výhody:
  - Jednoduchost užití
  - Růst spolehlivosti
  - Přívětivost
  - Odhalování rizikového chování

- Rizika:
  - Biometrika
  - Big Data u provozovatele
  - Vzniká nezávisle na vůli uživatele
  - Nové možnosti zneužití
  - Manipulace

Behaviorální biometriky - eliminace rizik

- Edukace:
  - Principy
  - Výhody/nevýhody

- Biometrika pod kontrolou:
  - Úprava chování
  - VPN

Odkaz pro kontrolu

It’s 2020. What Does Google REALLY Know About You?

https://www.vpnmentor.com/blog/what-does-google-know-about-you/

Máte nějaké dotazy?

Děkuji za pozornost

Ing. Vladimír Lazecký