NAKIT

Národní agentura pro komunikační a informační technologie, s. p.

Bezpečnostní opatření pro některé z oblastí kritické infrastruktury

Žijeme v době, kdy:

- Roste naše závislost na IT
- IT pronikají do oblastí, kde dříve nebyly
- Svět se stále více propojuje a vše se zrychluje
- Do internetu a sítí se připojují technologie a zařízení, která s tím nikdy v návrhu nepočítala – bezpečnost
- Takováto zařízení jsou často využívána v sítích KI
- Roste kvalifikovanost a technické schopnosti útočníků
- Do útoků se zapojují noví hráči
- Dochází k vývoji obchodních modelů i na hackerské scéně (CaaS)

Na co se bude zaměřovat kyberzločin v roce 2019

- **Útoky na dodavatelský řetězec** představují jeden z nejobávanějších druhů útoku, které v uplynulých dvou letech hackeři aplikovali. Kvůli tomu začaly firmy více přemýšlet o množství jednotlivých dodavatelů, se kterými spolupracují, a také intenzivněji řeší jejich zabezpečení.
- **Mobilní malware zůstane** na špici. Spousta hackerů do svých kampaní nezapomíná zařadit také komponenty zaměřené na mobilní zařízení, čímž se několikanásobně zvětšuje seznam potenciálních obětí.
- Počet takzvaných **IoT botnetů**, tedy ovládnutí prvků zapojených do takzvaného internetu věcí útočníkem, bude nezadržitelně stoupat. Varování před touto hrozbou se každoročně opakuje, ale právě proto nesmí být tato hrozba podceňována. IoT botnety neustále narůstají na množství a síle, a proto se z nich ve špatných rukách může stát velmi silná zbraň.
- **Spear-phishing** se v blízké budoucnosti stane velmi obávanou hrozbou. Data získaná prostřednictvím útoků na stránky sociálních sítí Facebooku, Instagramu nebo LinkedInu jsou nyní komukoliv přístupná na černém trhu. Nedávné obrovské úniky dat z databází různých sociálních sítí zvyšují úspěšnost hackerských útoků.

Zdroj: Kaspersky Lab

NAKIT

Reakce ČR na současný stav –> z 181/2014 Sb.

- Zákon o kybernetické bezpečnosti reaguje na situaci v KI od roku 2014
- Novely zákona z roku 2017:
  - Reagují na zkušenosti ze 3 let účinnosti zákona
  - Zavádějí soulad s evropskou směrnicí NIS
  - Definují nová odvětví:
    - 1. energetika,
    - 2. doprava,
    - 3. bankovnictví,
    - 4. infrastruktura finančních trhů,
    - 5. zdravotnictví,
    - 6. vodní hospodářství,
    - 7. digitální infrastruktura,
    - 8. chemický průmysl,
  - Zavádějí nový pojem základní služba, jejíž poskytování je závislé na sítích elektronických komunikací nebo informačních systémech a jejíž narušení by mohlo mít významný dopad na zabezpečení společenských nebo ekonomických činností v některém z těchto odvětví. (vazba na KII)
- 2019 – řešíme „cloudy“
- 2030 – ???

NAKIT

ZoKB – bezpečnostní opatření I.

- **§ 5**
- **(1)** Bezpečnostními opatřeními jsou
  - **a)** organizační opatření a
  - **b)** technická opatření.
- **(2)** Organizačními opatřeními jsou
  - **a)** systém řízení bezpečnosti informací,
  - **b)** řízení rizik,
  - **c)** bezpečnostní politika,
  - **d)** organizační bezpečnost,
  - **e)** stanovení bezpečnostních požadavků pro dodavatele,
  - **f)** řízení aktiv,
  - **g)** bezpečnost lidských zdrojů,
  - **h)** řízení provozu a komunikací kritické informační infrastruktury nebo významného informačního systému,
  - **i)** řízení přístupu osob ke kritické informační infrastruktuře nebo k významnému informačnímu systému,
  - **j)** akvizice, vývoj a údržba kritické informační infrastruktury a významných informačních systémů,
  - **k)** zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů,
  - **l)** řízení kontinuity činností a
  - **m)** kontrola a audit kritické informační infrastruktury a významných informačních systémů.

NAKIT

ZoKB – bezpečnostní opatření II.

- **(3)** Technickými opatřeními jsou
  - **a)** fyzická bezpečnost,
  - **b)** nástroj pro ochranu integrity komunikačních sítí,
  - **c)** nástroj pro ověřování identity uživatelů,
  - **d)** nástroj pro řízení přístupových oprávnění,
  - **e)** nástroj pro ochranu před škodlivým kódem,
  - **f)** nástroj pro zaznamenávání činnosti kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a administrátorů,
  - **g)** nástroj pro detekci kybernetických bezpečnostních událostí,
  - **h)** nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí,
  - **i)** aplikační bezpečnost,
  - **j)** kryptografické prostředky,
  - **k)** nástroj pro zajišťování úrovně dostupnosti informací a
  - **l)** bezpečnost průmyslových a řídících systémů.

Bude to v budoucnu jinak?

NAKIT

Proč je to důležité?

- Kybernetické útoky na KI každoročně přibývají a roste jejich závažnost
  - Např. v bankovnictví – 1/2018 110k unikátních hrozeb – 12/2018 již 170k
- V oblasti kybernetických útoků se stále více angažují státní aktéři – jiná motivace, jiné cíle, jiné možnosti financování
- Časté jsou ale i útoky s kriminální podstatou – typicky v poslední době Ransomware, ale časté jsou i krádeže dat
- Některé státy již zřizují speciální týmy na bezpečnost těchto systémů – specifičnost prostředí
- NATO a CCDCoE zařadily pravidelně do svých cvičení KB oblast „SCADA“ systémů; vazby mezi IT a OT

NAKIT

China's Social Credit System Barred Millions from Traveling in 2018

Over 23 million ticket purchases were blocked due to "social credit offenses."

Jacob Banas | March 2nd 2019

Do Not Pass Go

Your bags are packed, your rooms are booked, you're all set for your vacation; there's just one problem, the government has canceled your tickets.

As early as 2014, China began conceptualizing a Social Credit System (SCS), sort of like a credit score for citizen behavior where behaviors deemed good for society are rewarded with

Chinese Surveillance Is Literally Getting in Workers' Heads

Workers initially thought their employers could read their minds.

Kristin Houser | April 30th 2018

Feel like your boss is a bit of a micromanager, always looking over your shoulder? Be grateful that they're not peering *into your brain*.

That's now the case for a number of workers in China, the nation competing for the global superlative of Most Dystopian.

An "emotional surveillance" system is allowing supervisors to scrutinize employees' brainwaves for signs of

ARTIFICIAL INTELLIGENCE

Chinese Police Add Facial Recognition Glasses to Their Surveillance Arsenal

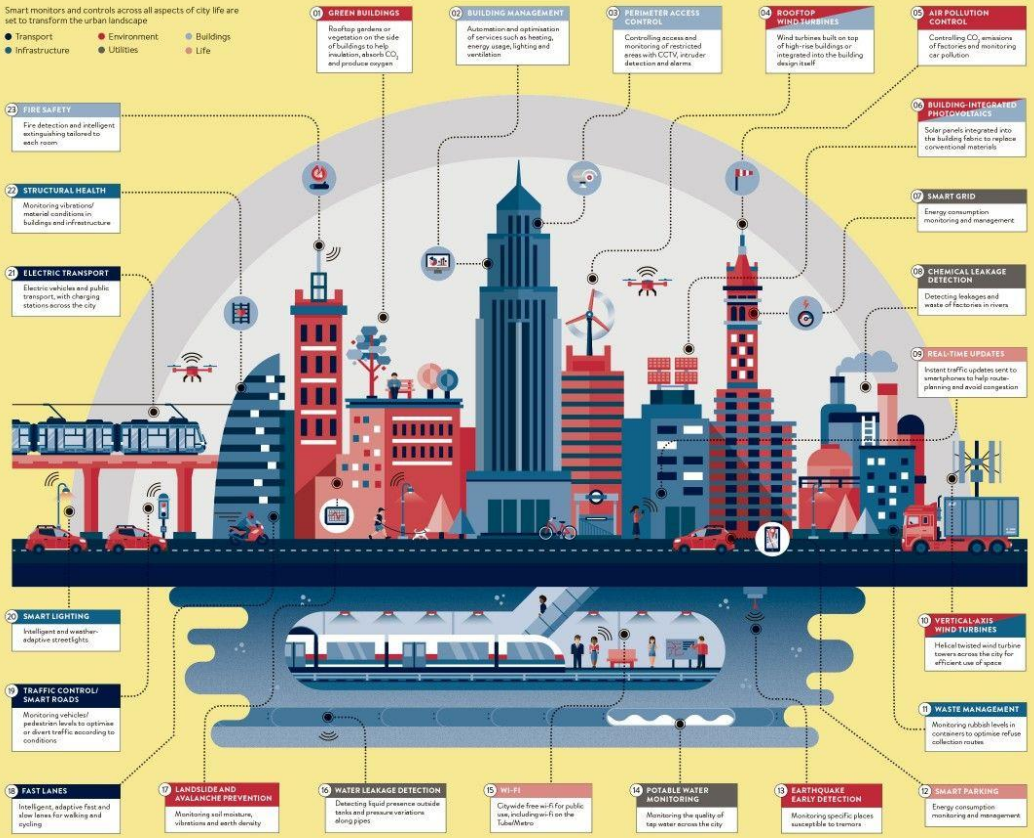
These glasses can scan a pre-loaded suspect database in just one tenth of a second.

Abby Norman | February 8th 2018

You've probably heard of Transitions lenses that can adapt to changing light conditions. Now, get ready for *facial recognition* lenses.

Police officers in Zhengzhou, China have been spotted wearing sunglasses equipped with facial recognition software that allows them to identify individuals in a crowd. These surveillance sunglasses were actually rolled out last year, but a recent report from China's QQ published a series of photos of the glasses in

Smart solutions for smart cities



NAKIT

NAKIT

NAKIT

Národní agentura pro komunikační a informační technologie, s. p.

Děkuji

Vladimír Rohel
Ředitel sekce Bezpečnost

+420 725 755 418

vladimir.rohel@nakit.cz