NAKIT

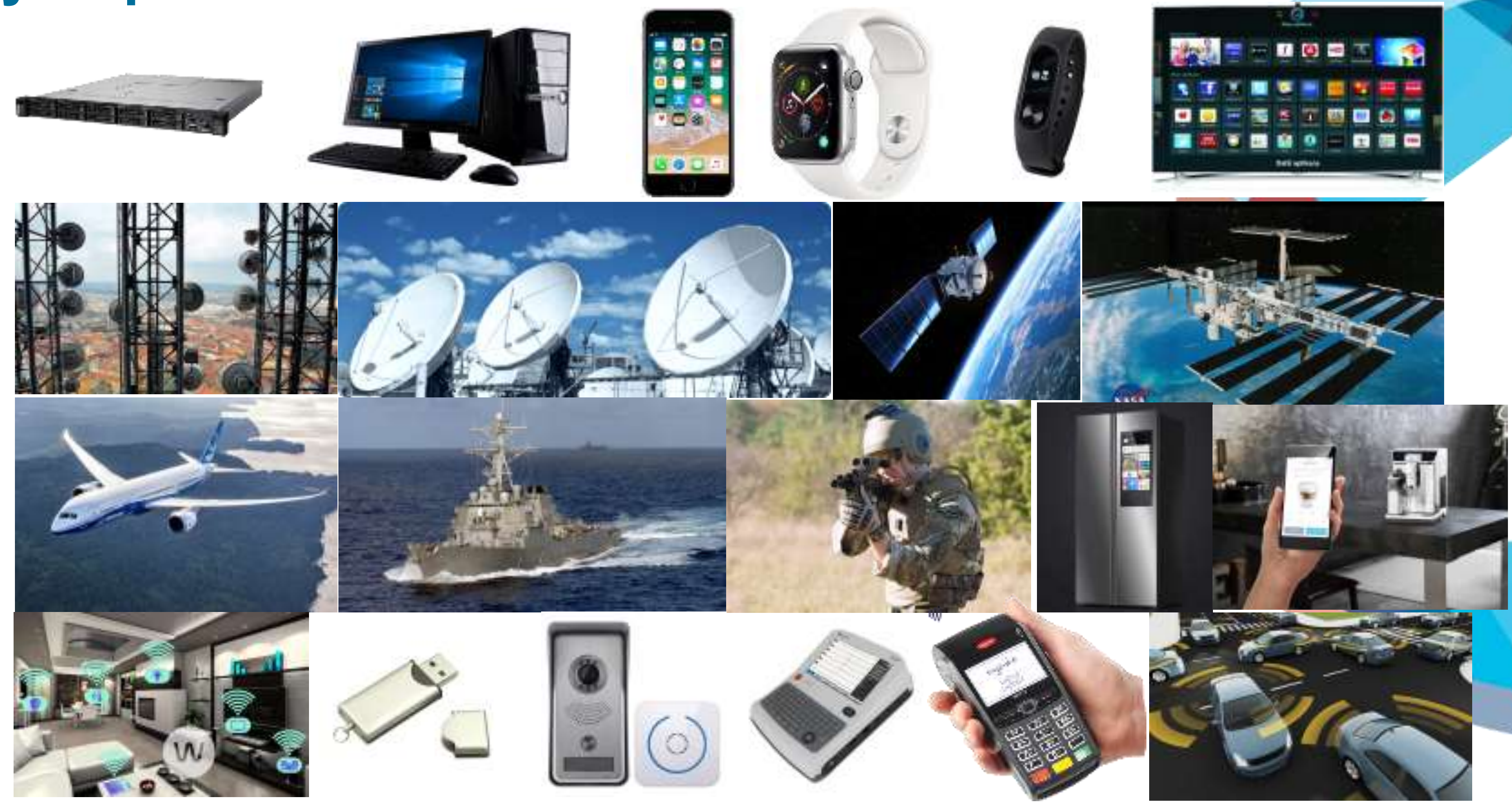
Národní agentura pro komunikační a informační technologie, s. p.

Kyberbezpečnost a rizika spojená s používáním spotřební elektroniky

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 – co bezpečnost?
- Takováto zařízení jsou často využívána i 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)

Kyberprostor



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

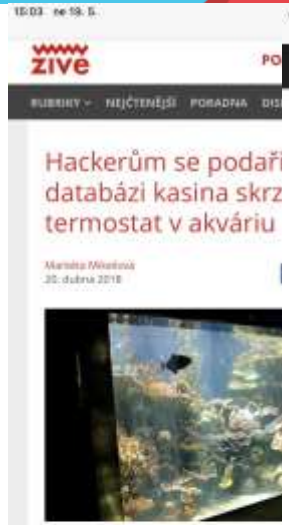
Je důležité to řešit nyní?

- 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 velmi časté jsou i krádeže dat
- Sociální inženýrství, analytická práce = začátek cíleného útoku

Stuxnet objeven 2010

- Některé státy již zřizují speciální týmy na bezpečnost „neIT“ systémů – specifičnost prostředí
- NATO, CCDCOE i EU zařadily pravidelně do svých cvičení KB oblast „SCADA“ systémů, vazby mezi IT a OT

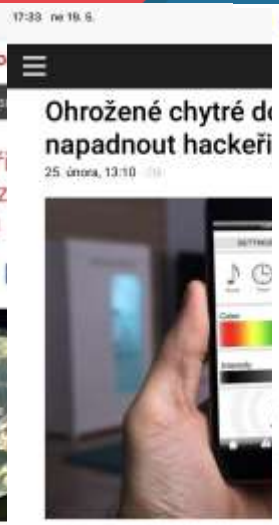
NAKIT



zive

Hackerům se podaří
databázi kasina skrz
termostat v akváriu

Marketa Mikesova
20. dubna 2018



Ohrožené chytré d
napadnout hackeři

25. února, 13:10

Dvě z pěti českých a slovens
věcí jsou vystaveny kyberne
další síťová zařízení připojen
i bezpečnostní kamery nebo

„Lidé chtějí používat chytré televiz
chůvičku svého dítěte do domácí
stačí jediné slabé zabezpečené za
přistupovat k ostatním zařízením
nahrávání videí a hlasů," uvedl pr
výsledky studie na veletrhu Mobil

Ze zprávy Avast Smart Home Repo
domácích sítí po celém světě, vypl
má připojených více než pět chytr
připojené zařízení.

ARTIFICIAL INTELLIGENCE

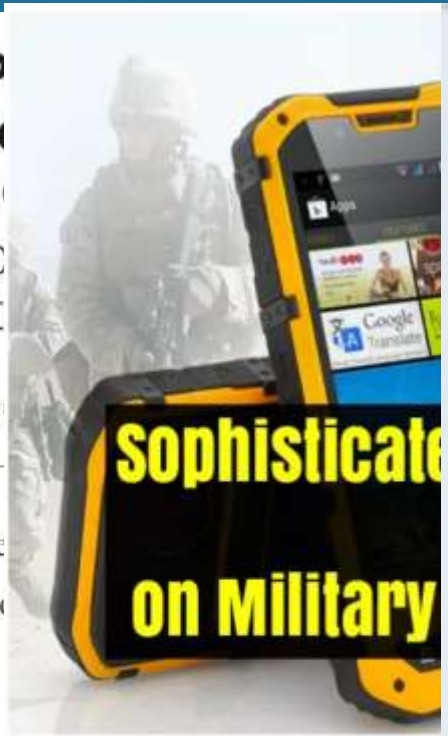
Chinese P
Recognitio
Surveillan

These glasses c
database in just

Abby Norman | February

You've probably he
changing light cone
lenses.

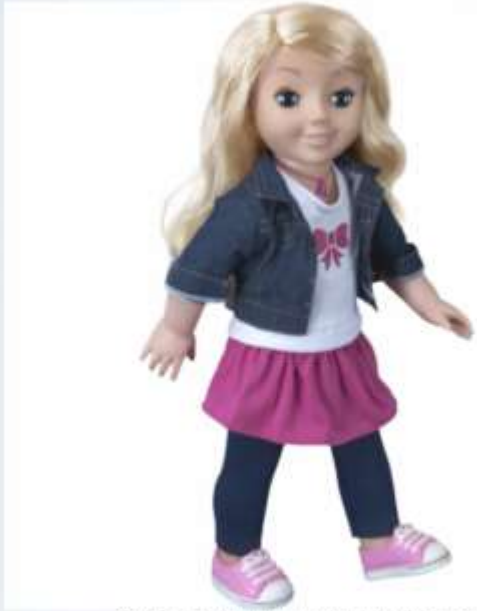
Police officers in Z
sunglasses equippe
them to identify in
sunglasses were ac
from China's QQ p



A few days before the Israeli securit
installed a sophisticated spyware in
various sensitive information such a

Spyware distributed through fake W
spread through the Google play stor

Cayla – The Illegal Espionage Apparatus



Source: ParentingHub https://parentinghub.co.za/2014/10/my-friend-cayla/

With waist-length golden hair and a voice designed to warm a child's heart, Cayla has brought delight to millions of children throughout Germany. In reality, she's an "illegal espionage apparatus" that must be destroyed immediately, according to Germany's Federal Network Agency.

Once hackers are in control of this Wi-Fi – enabled interactive doll, they can use its cameras and microphones to see and hear whatever Cayla does, allowing hackers to track their location or potentially heist profits from the local street-side lemonade stand. Most importantly, when the security on these Internet-connected devices are neglected

China's S
Barred Mi
in 2018

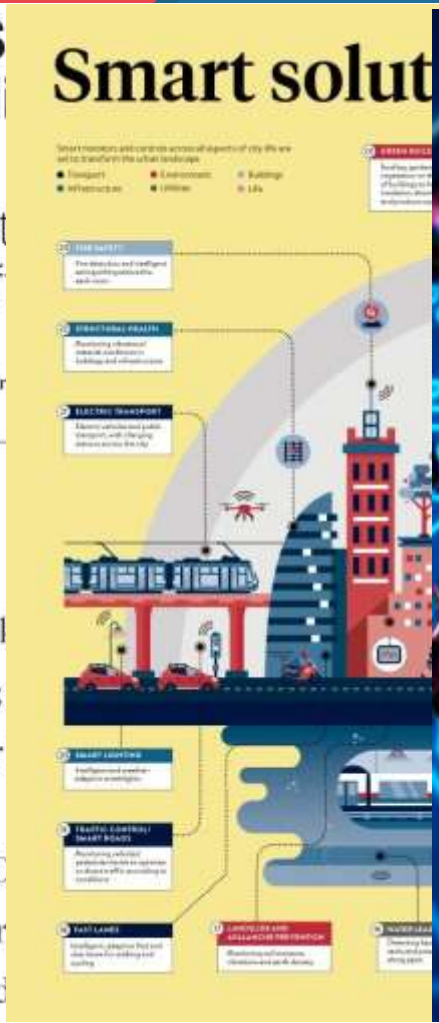
Over 23 million t
"social credit of

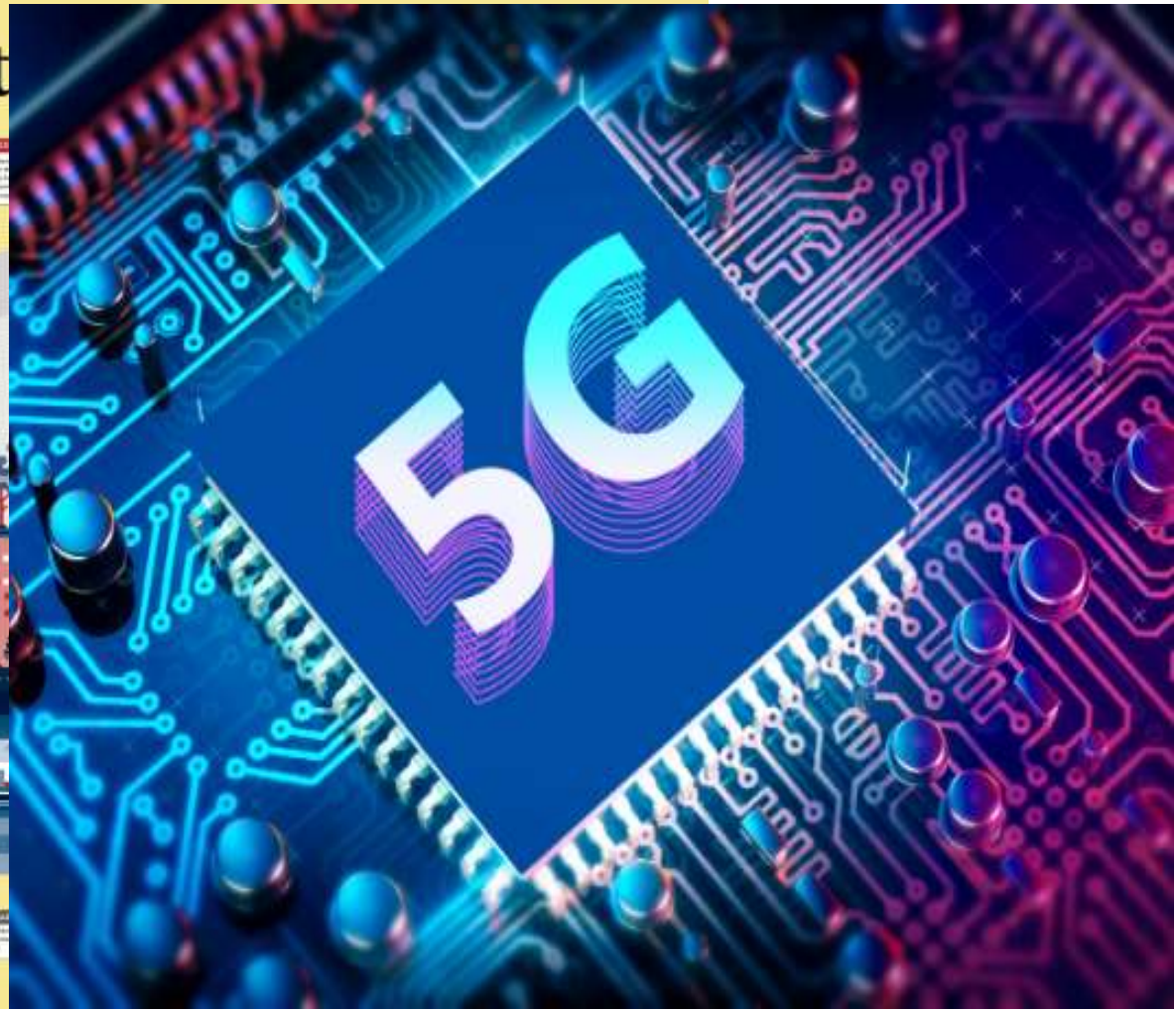
Jacob Banas | March 2r

Do Not Pass Go

Your bags are pacl
for your vacation;
has canceled your

As early as 2014, C
System (SCS), sor
where behaviors d





AI for Cyber Security: How AI prevents future cyberattacks?

Many routinely describe cybersecurity as a game of cat-and-mouse. That is, hackers and cybercriminals are always one or two steps ahead of law enforcement as the latter continually pursue the former's ever-advancing plans to commit data theft, property damage, other security breaches—often spotting breaches long after such knowledge is helpful. The cybersecurity cat remains slower and unab to predict the mouse's next move. And the cybercriminal mouse evades capture. How, then, can cybersecurity anticipate the cybercriminal's next move?

This is where cybersecurity analytics comes in, a practice one can think of as cybersecurity mousetraps. This article takes a look at h measures such as analytics and artificial intelligence allow cybersecurity teams to anticipate in advance an evasive cybercriminal's ne move.

Cybersecurity is often thought of as a defensive practice that largely happens after the fact. First a security breach is detected, and t a cybersecurity team is mobilized in order to track down the source, type, and scale of the damage. Only then can an offender be apprehended and appropriate resources put into place. This paradigm, however, has become reshaped and rethought through recent breakthroughs in cybersecurity. Specifically, artificial intelligence and big data are being leveraged to counteract cybercrime through smart cybersecurity countermeasures. In essence, such approaches—not unlike the scenarios found in Minority Report (2002) or Pers of Interest (2011-16)—can actually prevent cybercrime by anticipating it in advance.

For cybersecurity teams, the ability to foresee attacks and provide proactive countermeasures is critical in the fight against cyberattacks. A key part of building this knowledge involves understanding just what is at stake. What assets are potentially vulnerab to attack? What could hackers possibly target? According to Duo Helmbrecht, executive director for the EU Agency for Network and Information Security (ENISA), "Identification of threats and their dynamics in cyber-space is key to understanding asset exposure an risks."[1] Knowing what is at risk, in other words, is the first step in knowing what kinds of attacks will be made. In terms of financial damage, experts have estimated that the average US company pays upwards of $15 million per year, and that is only in cybercrime losses.[2] But in addition to how much it costs in damage, security teams need to know how, where, and when an attack will take place.

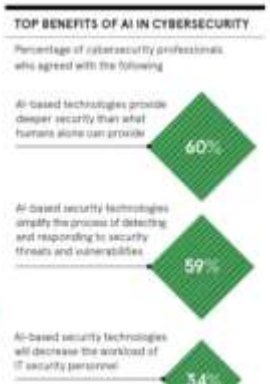
RACONTEUR

AI has shaken up the cybersecurity industry, with automated threat prevention, detection and response revolutionising one of the fastest growing sectors in the digital economy.

> Hackers are using AI to speed up polymorphic malware, causing it to constantly change its code so it can't be identified

However, as is so often the case, there's a dark side. What if cybercriminals get their hands on AI, and use it against public and private sector organisations?

The more AI cybersecurity solutions, the more tempting for hackers



"The edge in cyberdefence is speed. AI is transforming cyberdefence, allowing businesses to detect evermore complex threats from evermore sophisticated attackers," says Andre Pienaar, founder of C5 Capital.

Nevertheless, the more AI security solutions, the more cybercriminals will adopt the technology; it's a case of fighting fire with fire. Newton's Third Law describes the situation aptly: for every action, there is an equal and opposite reaction.

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