# Kybernetická rizika na robotizovaných pracovištích s použitím umělé inteligence a možná bezpečnostní opatření
# Cyber Risks in Robotic Workplaces Using Artificial Intelligence and Possible Safety Measures

**Ing. Pavel Šuška**
**Ing. Aleksandr Kochnev**
VŠB-TUO, Fakulta bezpečnostního inženýrství
Lumírova 13, 700 30 Ostrava - Výškovice
pavel.suska@vsb.cz, aleksandr.kochnev@vsb.cz

**Abstrakt**

Cílem článku je seznámit osoby zabývají se BOZP s kybernetickými riziky, která vyplívají při používání robotických pracovišť vybavených umělou inteligencí. Práce v první části poukazuje na zvyšující se množství kybernetických útoků a možná a reálná kybernetická rizika, jež mají za následek pracovní úrazy. Druhá část se zabývá možnými cestami vniku útočníka do systému organizace. Třetí část popisuje základní bezpečnostní opatření, která vedou ke snížení kybernetických rizik.

**Klíčová slova**

Kybernetická rizika, robotika, umělá inteligence, SCADA, ICS.

**Abstract**

The aim of this article is to acquaint people dealing OSH with cybernetic risks that arise in use of robotic workplace equipped with artificial intelligence. In the first part of article showing of an increasing number of cybernetic attack and a possible and real cybernetic risk that result in accidents at work. The second part of article include a possible way of the attacker's intrusion into the organization's system. The third part of article describes the basic security measures that lead to the reduction of cybernetic risks.

**Keywords**

Cybernetics, robotics, artificial intelligence, SCADA, ICS.

## Úvod

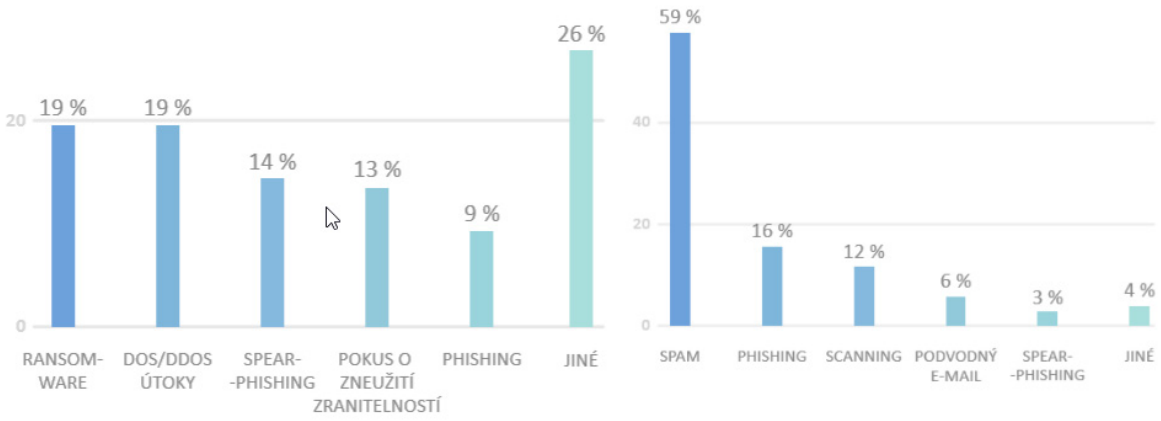
Mezi průmyslově nejvyspělejší země v EU patří Česká republika s téměř 40 % podílem přidané hodnoty v ekonomice. Z toho více než pětina produkce připadá na automobilové odvětví. Vláda České republiky se zavázala, že se během dvanácti let zařadí mezi inovační lídry Evropy a stane se zemí technologické budoucnosti. Jeden z inovačních kroků je národní strategie pro umělou inteligenci (dále jen AI) [1].

Stejně jako každá technologie má i umělá inteligence ambivalentní charakter. Na jednu stranu AI může přinést významné možnosti rozvoje pracoviště a růstu produktivity. Na druhou stranu může AI přinést mnoho nových výzev v bezpečnosti a ochrany zdraví při práci zejména v oblasti kybernetických, psychosociálních a mechanických rizik [1], [2]. Je nutné zejména zdůraznit kybernetická rizika, která vyplývají z užívání umělé inteligence skupinami zločinců, teroristů, a ztráty, jež může zločinné užívání způsobit v průmyslu.

Útoky mohou být zaměřené převážně na průmyslové podniky obsahující velké množství nebezpečných chemických látek s cílem vyvolat závažnou havárii, která ohrozí obyvatelstvo, životní prostředí a majetek. Takové havárie mohou způsobit smrt tisíců lidí, otrávit nespočet vodních živočichů a kontaminovat půdu. Zneužitá AI může usnadnit teroristům přístup k průmyslovým prostředím s nebezpečnými látkami. Mezi možné scénáře patří i zneužití robotického pracoviště vybaveného AI, které může teroristům usnadnit přístup k nebezpečným látkám nebo vyvolat vznik závažné havárie. Další možné zneužití umělé inteligence spočívá v ovládnutí autonomních dopravních prostředků, které převážejí nebezpečné látky nebo výbušniny, a jejich úmyslná havárie. Taková havárie může mít velmi tragické následky.

## Současná situace v oblasti kybernetických rizik

Závažnost kybernetických rizik neustále stoupá, tento fakt také podporuje zjištění z kontrolní akce NKÚ (Nejvyššího kontrolního úřadu). Z kontrolní akce vyplývá, že od roku 2017 do poloviny roku 2020 došlo k 916 kybernetickým incidentům, které byly hlášeny vládnímu CERT (*Computer Emergency Response Team*). Z toho 31 % kybernetických incidentů připadlo na první polovinu roku 2020 [3]. V roce 2020 byl nejčastějším typem útoku v České republice spam, phishing a skenování vnějších sítí. Naopak nejméně častým typem útoku byl sniffing (skenování vnitřní sítě), jak je uvedeno na obrázku obr. 1 vpravo. Nejzávažnějším typem útoku v roce 2020 byl ransomware, DoS/DDoS (*Denial of Service*), jak je uvedeno na obr. 1 [4].




Obr. 1 Nejčastější a nejzávažnější typy útoků [4]

**Kybernetická rizika v praxi**

S rostoucím počtem kyberútoků roste i množství zneužitých robotických pracovišť, která jsou vybavena umělou inteligencí. Takové zneužití může mít za následek pracovní úrazy zaměstnanců v areálu průmyslových podniků. V následujících odstavcích jsou popsány reálné úrazy, které vznikly v důsledku kyberútoku.

V květnu roku 2015 zemřel v americké automobilce nacházející se v Cincinnati zaměstnanec na následky rozdrcení lebky. Toto úmrtí bylo způsobeno neočekávaným restartováním robotického systému. Vyšetřování ukázalo, že robotická platforma byla infikována malwarem, který přepsal a poškodil příkazy robotické platformy [5].

V prosinci roku 2017 bylo v americkém obchodním centru v Sillicon Valley přejeto batole autonomním robotickým mycím strojem. Z vyšetřování vyplynulo, že bezpečnostní příkazy byly přepsány hacknutím, jež provedla nezletilá osoba za použití skriptu staženého z internetu [5].

**Průmyslový systém ICS/SCADA**

Mezi nejčastěji cíle kybernetických útoků mezi roky 2019 a 2020 patří digitální služby (e-mail, sociální platformy), průmysl, zdravotnictví a státní správa. Frekventované typy útoku na průmysl jsou útoky na průmyslové řídicí systémy a systémy pro řízení, dohled a sběr dat [6].

Průmyslové řídicí systémy (ICT) a systém pro řízení, dohled a sběr dat (SCADA) jsou počítačové systémy, které se zaměřují na dohled, monitorování a sběr dat v reálném čase [7].

SCADA a ICT systémy lze využít v sektorech, kde je nutné monitorovat a kontrolovat systém nebo strojní zařízení. Dále se systém SCADA běžně používá k automatizaci složitých průmyslových procesů. SCADA systémy lze použít např. ve výrobě, kde jsou systémy SCADA použity pro regulaci výrobních linek, monitorování kvality a robotických zařízení, jako je například robotická paletizace. V případě robotické paletizace řídí SCADA systém programy robotů z databáze, která obsahuje velké množství programů pro plnění palet v závislosti na tvaru, velikosti a množství zboží [8].

**Bezpečnostní riziko**

Systém SCADA bývá fyzicky oddělen od informačních a komunikačních sítí podniku a používá izolované lokální sítě, virtuální lokální sítě nebo jinou formu síťové infrastruktury. Ve většině případů potřebuje SCADA systém přístup k ostatním sítím (internet), ať už pro účely podpory třetích stran (výrobce, dodavatel), nebo za účelem poskytnutí nashromážděných dat.

Právě připojení k internetu a ostatním sítím může skýtat bezpečnostní rizika, jež lze rozdělit na dvě kategorie:

- cílené útoky APT (Advanced Persistent Threat) - pokročilá persistentní hrozba,
- interní útoky [9], [10].

Cílené útoky APT jsou pečlivě vytvořené útoky proti konkrétnímu cíli. Používají různé způsoby, jak proniknout ke svému cíli. Mezi tyto metody patří například shromažďování informací a chování lidí na internetu. Tyto informace slouží k vytvoření škodlivých stránek, které nalákají cílové osoby k jejich návštěvě a stáhnutí škodlivého kódu (malware) [11].

Interní útoky jsou dalším způsobem proniknutí škodlivého kódu do vnitřní sítě podniku. Při tomto útoku dochází k vnesení infikovaného média (přenosné HDD, mobil) a jeho připojení do místní sítě. Tento útok může být proveden neúmyslně, nebo úmyslně [12].

**Doporučení ke snížení bezpečnostních rizik**

SCADA a ICT byly tradičně uzavřené systémy navržené pro funkčnost, bezpečnost a spolehlivost a jejich fyzické oddělení od informačních a komunikačních sítí. Zvýšená konektivita prostřednictvím standardních IT technologií je vystavila novým hrozbám, na něž nejsou dostatečně vybavena (například červi, viry, DDoS) [9], [10].

V následujících odstavcích jsou sepsána základní bezpečnostní opatření, která přispívají ke snížení kybernetických rizik.

***Firewall***

- Chraňte připojení mezi systémy řízení procesů a další systémy pomocí brány firewall.

***Vzdálený přístup***

- Udržujte seznam všech vzdálených připojení.
- Zaveďte vhodné mechanismy autentizace, jako je silné ověřování (dvoufázové ověřování), pro všechna připojení ke vzdálenému přístupu.
- Vhodně zabezpečte všechny počítače se vzdáleným přístupem (antivirus, firewall).
- Proveďte bezpečnostní kontroly všech třetích stran, které mají vzdálený přístup k řídicím systémům.

***Antivirus***

- Chraňte systémy řízení procesů antivirovým softwarem na všech serverech a pracovištích.
- Před instalací antivirových softwarů získejte od dodavatelů systémů řídicích procesů instrukce o konfiguraci, kompatibilitě [13].

**Závěr**

Pokrok v oblasti digitalizace, robotizace a implementace umělé inteligenci nelze zastavit a některé výše zmíněné roboty a prvky umělá inteligence jsou již součást naší reality. S rostoucí digitalizací a automatizací v průmyslu poroste i množství kybernetických útoků. Bohužel nejde na sto procent zajistit kybernetickou bezpečnost, ani odstranit všechna rizika plynoucí ze zavedení robotů s umělou inteligenci. Tyto útoky mohou mít za následek odcizení dat, špionáž, vznik závažné havárie nebo pracovní úrazy. Avšak díky včasnému provedení kvalifikovaného hodnocení rizik na základě možných scénářů, za pomocí modernizované metodiky hodnocení rizik lze zajistit přípravu a rizika zmírnit na přijatelnou úroveň. Je nutné podotknout, že roboty a umělá inteligence při zodpovědném použití nejsou jen hrozbou, ale zároveň nástrojem pro zajištění bezpečnosti a ochrany zdraví zaměstnanců na budoucích modernizovaných pracovištích.

**Použitá literatura**


[1] ATLE, R.; BJøRNARV, S.; STOLEN, K.: *Cyber-Risk Management*. Springer International Publishing, 2015. ISBN 978-3-319-23570-7.

[2] RSA WHITE PAPERCYBER RISK APPETITE: Defining and Understanding Risk in the Modern Enterprise. *Rsa* [online]. 2016 [cit. 2021-05-05]. Dostupné z: https://www.rsa.com/content/dam/en/white-paper/cyber-risk-appetite.pdf.

[3] Kontrolní závěr z kontrolní akce 19/26: Budování kybernetické bezpečnosti České republiky. *Nejvyšší kontrolní úřad* [online]. Česká republika, 2019 [cit. 2021-05-05]. Dostupné z: https://www.nku.cz/assets/kon-zavery/k19026.pdf.

[4] ŘEHKA, K.: *Zpráva o stavu Národní úřad pro kybernetickou a informační bezpečnost ZPRÁVA O STAVU KYBERNETICKÉ BEZPEČNOSTI ČESKÉ REPUBLIKY ZA ROK 2020.* 1. Praha: NÚKIB, 2020.

[5] BHARDWAJ, A.; AVASTHI, V.; GOUNDAR, S.: Cyber security attacks on robotic platforms. *Network Security* [online]. 2019, 2019(10), 13-19 [cit. 2021-05-05]. ISSN 13534858. Dostupné z: doi:10.1016/S1353-4858(19)30122-9.

[6] Main incidents in the EU and worldwide: ENISA Threat Landscape. *ENISA* [online]. Attiki, Greece, 2020, 7-10 [cit. 2021-09-24]. Dostupné z: doi:10.2824/552242.

[7] Co je to SCADA?. *Promotic.eu* [online]. Tavičská 845/21 703 00 Ostrava-Vítkovice, 2012 [cit. 2021-09-24]. Dostupné z: https://www.promotic.eu/cz/pmdoc/WhatIsPromotic/WhatIsScada.htm.

[8] Case study: SCADA system puts robots on a roll. *Processengineering* [online]. 2012 [cit. 2021-09-24]. Dostupné z: https://processengineering.co.uk/article/2023061/case-study-scada-system-puts-robots-on-a-rollv.

[9] Bezpečnost průmyslových sítí a systémů SCADA/ICS. *Systemonline* [online]. 2001 [cit. 2021-09-24]. Dostupné z: https://www.systemonline.cz/rizeni-vyroby/bezpecnost-prumyslovych-siti-a-systemu-scada-ics.htm?mobilelayout=false.

[10] Kyberútoky na kritickou infrastrukturu. *Systemonline* [online]. [cit. 2021-09-24]. Dostupné z: https://www.systemonline.cz/energetika-a-utility/kyberutoky-na-kritickou-infrastrukturu-1.htm).

[11] ZHOUV, X.; XU, Z.; WANG, L.; CHEN, K.; CHEN, C.; ZHANG, W.: APT Attack Analysis in SCADA Systems. *MATEC Web of Conference*s [online]. SIMMA, 2018, 173 [cit. 2021-09-24]. ISSN 2261-236X. Dostupné z: doi:https://doi.org/10.1051/matecconf/2018173.

[12] MANCUSO, F.; STRANG, V.A.J.; FUNKE, G.J.; FINOMORE, V.S.: Human Factors of Cyber Attacks: A Framework for Human-Centered Research. *Sage journal* [online]. SAGE Publications [cit. 2021-09-24]. Dostupné z: doi:https://doi.org/10.1177/1541931214581091.

[13] Good Practice Guide Process Control and SCADA Security. *Https://niscc.info/* [online]. niscc [cit. 2021-09-24]. Dostupné z: https://www.controlglobal.com/assets/Media/MediaManager/wp_06_niscc_scada.pdf.