Abstrakt

Tato práce má za cíl prozkoumat riziko, které s sebou nese nezabezpečení Armády České republiky na sociálních sítích, chování uniformovaných příslušníků a jejich identifikace na sítích. Ruská agrese na Ukrajině a hacking českých zdravotnických zařízení opět poukázali na roli, kterou hraje kyberbezpečnost v moderním světě a to, že právě člověk je nejslabším článkem v rámci zabezpečení.

Tato případová studie se proto snaží definovat ideální typy chování vojáků na sociálních sítích a následně analyzovat rizika, která jednotlivé typy představují. S tímto cílem práce nejprve představuje důležité informace nutné k plnému pochopení rozsáhlé tématiky kyberbezpečnosti na sociálních sítích. Dále práce definuje několik ideálních typů a jejich stavební složky, které slouží pro kategorizaci vojáků na sociálních sítích a ty následně analyzuje. Autor dochází k závěru, že každý definovaný ideální typ má se sebou inherentně spojené problematické chování a nese tak míru rizika pro Armádu České republiky. Nejrizikovějšími byly shledány ideální typy přítomného uživatele a rodinného příslušníka.

Klíčová slova

OSINT, SOCMINT, NATO, Armáda České republiky, Kyberbezpečnost, Bezpečnost, Sociální sítě, Analýza ideálního typu, Sociální inženýrství

Název práce

Nezabezpečení příslušníků Armády České republiky na sociálních sítích