# Desatero kyberbezpečnosti #1

## Počítačová bezpečnost aneb nebezpečné e-maily

*V prvním článku z tohoto cyklu se dozvíte, jak hackeři úspěšně využívají nové viry a sociální inženýrství k napadení počítačů, přestože existují bezpečnostní filtry a antiviry.*

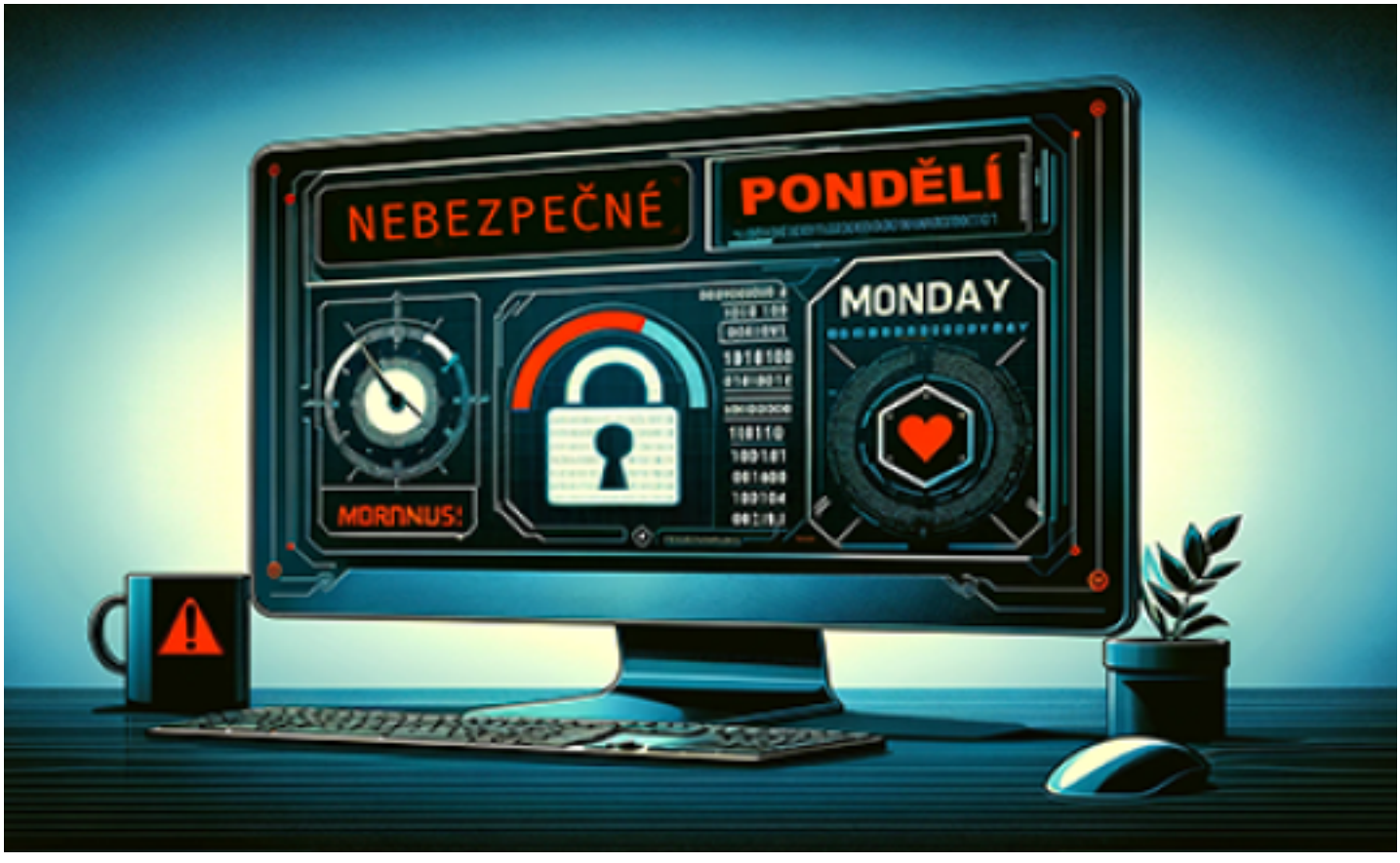
E-mailová komunikace je dnes neodmyslitelnou součástí našich soukromých i pracovních životů. K některým z nás přilétají tito moderní poštovní holubi několikrát denně, u jiných se za den vystřídá celé hejno.

Při používání pracovního e-mailu se většinou spoléháme na bezpečností opatření, která nás chrání před nežádoucími hrozbami. Všechny e-maily, které nám do univerzitní schránky přicházejí, jsou zkontrolované antispamovými a antivirovými filtry. Pro ještě větší ochranu nám na našich počítačích běží další antivirový program, který každý otevřený e-mail ještě jednou zkontroluje. **Nicméně i přes všechna tato bezpečnostní opatření jsou e-maily jedním ze základních nástrojů kybernetických útoků.**

## Nebezpečná kreativita počítačových hackerů

Denně vznikají **nové varianty virů a podvodných e-mailů**, které se antivirové programy musí učit rozeznávat. Ačkoliv se antivirové programy učí rychle, vždy to trvá nějaký čas (někdy i několik hodin) než se program naučí nové hrozby identifikovat. Hackerům tak vzniká okno, během něhož mohou propašovat nový virus skrz e-mail s přílohou, ještě předtím, než je bezpečnostními filtry odhalen.

Tento jev, známý jako **"nebezpečné pondělí"**, využívá časování nebezpečných e-mailů na brzké ranní hodiny v pondělí, aby na začátku pracovní doby byly už e-maily ve schránkách. Toto načasování limituje možnost administrátorů reagovat na nebezpečí a zvyšuje tak počet poškozených, kteří přílohu e-mailu otevřou.




# Pozor na manipulaci formou „sociálního inženýrství“

Schopný hacker dokáže **přesvědčivým způsobem** manipulovat příjemce k provedení akce, která spustí infekci. Říká se tomu **„sociální inženýrství“** a jde o kombinaci **přesvědčivosti a nátlaku**, kdy útočníci se často vydávají za legitimní entity. Odesílatel se například vydává za "IT CUNI Support" a píše, že když nějakou akci neuděláte do 10 minut, "tak přijdete o přístup ke svému účtu, prémie, stravenky a dva dny osobního rozvoje". Tato oblíbená metoda sociálního inženýrství může zmanipulovat jakéhokoliv příjemce, aby poslal své jméno, heslo, anebo PIN k platební kartě. Dále může přesvědčit příjemce, aby na svůj počítač nainstaloval aplikaci z podezřelého zdroje, spustil ji, a podle návodu v e-mailu ještě umlčel „protestující“ antivirus.
Z toho všeho vyplývá, že přestože jsou technická opatření důležitá, konečnou instancí a poslední obrannou linií jste právě **vy a vaše obezřetnost**. Vaše obezřetnost spočívá ve stálé ostražitosti a vědomí ohledně potenciálních hrozeb, abyste mohli účinně bránit svůj počítač a celou organizaci před kybernetickými útoky.

Chcete-li se o tématu dozvědět víc, navštivte web Kyberbezpečnost na Univerzitě Karlově a v článku Nebezpečí v e-mailech se můžete podívat na vzorky skutečných phishingů , zavirovaných příloh , pokusů o vydírání a pokusů o podvod , kterými se nás - zaměstnance univerzity - někdo pokusil v poslední době napálit.

Na článku spolupracovali:
Ing. Vladimír Horák, vedoucí CSIRT (Computer Security Incident Response Team)
Zora Jašková, DiS., Ústav výpočetní techniky

Pokud máte k článku připomínky, korektury, nebo dotazy, kontaktujte nás prosím na e-mailu: internikomunikace@ruk.cuni.cz .