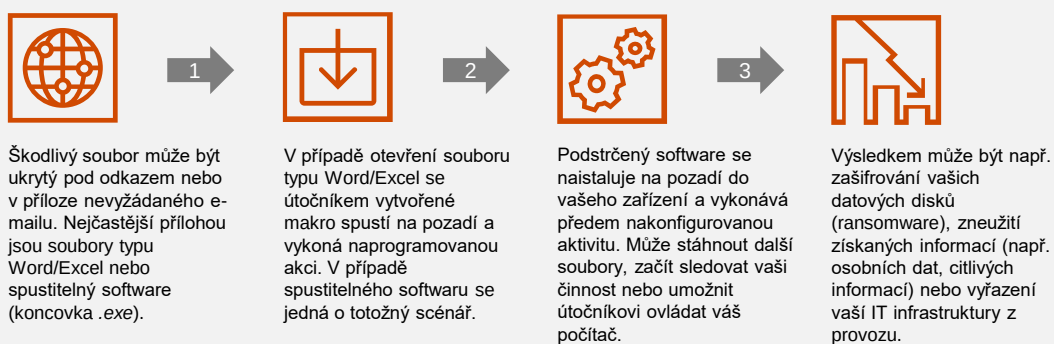


Kybernetický útok

Víte, jakou roli v případě kybernetického útoku máte vy? Tu nejdůležitější. S čím dál pokročilejšími nástroji, které chrání společnosti před kybernetickými útoky, si útočníci raději vybírají ten nejzranitelnější faktor – lidský. Proto se vám v emailových schránkách objevují nevyžádané e-maily s podezřelými odkazy a přílohami.

Jak takový útok může vypadat?



1. Útočník zasílá nejčastěji jeden typ e-mailů na více e-mailových adres a vyčkává, kdo si soubor stáhne/klikne na odkaz a naistaluje do svého zařízení.
2. Škodlivý software se instaluje do vašeho zařízení a pokračuje v tom, k čemu byl naprogramován. Podezřelá aktivita se nemusí stát okamžitě, jelikož škodlivý software se může projevit/aktivovat až s odstupem času.
3. Software poté může provést změny, či odesílat data z vašeho zařízení na útočníkův server. Ukradená data mohou být poté zpeněžena, či použita jako nástroj pro vydírání.

Jak se takovému útoku bránit a snížit jeho dopady?

Ověřte si e-mail s odkazy/přílohami <https://drive.google.com/download-photo.sytez.net/AONh1e0hVP>

Najetím myši na odkaz se zobrazí opravdová adresa odkazu. Pokud se vám bude zdát podezřelá (např. bude dlouhá a nesrozumitelná nebo nebude směřovat na oficiální adresu), buďte opatrní a neklikajte.

V případě podezřelé situace ihned kontaktujte své IT kolegy

Vaši kolegové vám ihned pomůžou a zjistí, zda se jednalo o opravdový útok či jen o SPAM (nevyžádaný e-mail). Podezřelý e-mail můžete většinou nahlásit přímo v e-mailovém klientovi pomocí ikony k tomu určené.

Sdělte svým kolegům vaši zkušenost

Varováním vašich kolegů před škodlivým e-mailem snížíte pravděpodobnost, že budou úspěšně napadeni útočníkem.

Jak vám můžeme pomoci?

Pokud máte nějaké dotazy ohledně tohoto vydání, neváhejte se na mne obrátit. Rád vám poradím i v dalších oblastech kybernetické bezpečnosti.



Oddělení IT Bezpečnosti