
# SOPHOS SANDSTORM: NOVÝ STANDARD SÍŤOVÉ BEZPEČNOSTI

Sophos Sandstorm je nová technologie pro Sophos UTM. Je dostupný od verze UTM 9.4. Zjednodušuje a vylepšuje UTM zabezpečení proti malware přidáním cloudového sandboxingu.

V současné praxi je běžné, že administrátor zavádí opatření proti malware v e-mailových přílohách nebo stahovaných souborech. Obvykle je to vyloučením typů některých spustitelných příloh a omezením stahování pro určitou skupinu uživatelů, a také omezením zdroje, z kterého lze data stahovat.

Taková ochrana není dokonalá, stále je nutná spolupráce poučeného uživatele. Není totiž možné zakázat úplně všechny potenciální zdroje infekce. Mnohé firmy potřebují k práci technologie, jako jsou MS Office makra, JavaScript, Flash atd.

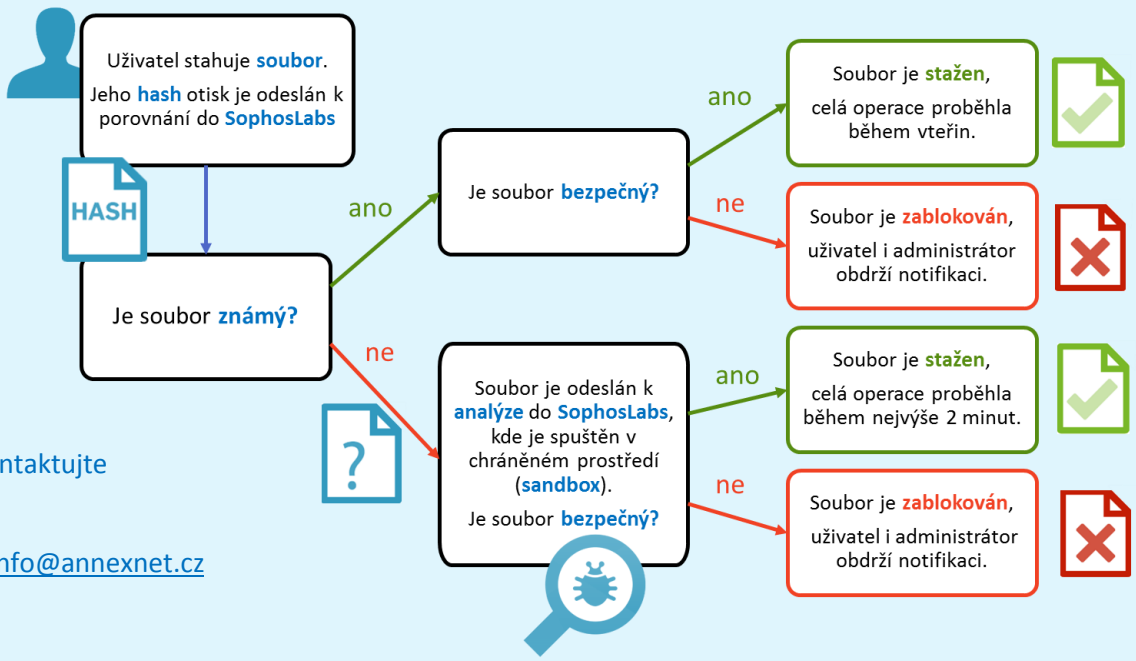
Dle společnosti Sophos je **sandboxing** funkcí, která by se měla stát standardem zabezpečení firemní infrastruktury podobně jako IPS/IDS, aplikační kontrola, URL filtering a další dnes již standardní nástroje **Sophos UTM** řešení. Pouhá antivirová kontrola na koncových stanicích již dnes není dostačujícím řešením.

## Sophos Sandstorm v praxi: Virus zvaný locky

Nový typ malware z rodiny ransomware jménem **Locky** se šíří podvrženým dokumentem (doc, xls atd.), který při otevření navrhne spustit makra. Po odsouhlasení nepozorného uživatele se nainstaluje na počítač a dojde k rozeslání dle kontaktů v počítači na další zařízení v okolí. Lockyho e-maily jsou šířeny prostřednictvím sofistikovaných kampaní, lokalizované s perfektní češtinou s použitím sociálního inženýrství na vysoké úrovni. Podobné soubory lze najít také na veřejných úložištích v office souborech, tvářící se jako návody, postupy atd.

**Sophos Sandstorm** pomocí spuštění v chráněném prostředí (sandboxing) odhalí škodlivou povahu souboru s makry. Včas zabrání jeho stažení a následné infekci sítě. Zároveň informuje administrátora o tom, kdy, kde a jak došlo k pokusu o stažení infikovaného souboru.

## Jak pracuje Sophos Sandstorm




Pro více informací kontaktujte

**Annex NET, s.r.o.**

+420 212 341 541 | info@annexnet.cz

www.annexnet.cz