Vyděračské útoky (tzv. ransomware, který šifruje důležité soubory na počítači), kterým věnují média posledních 24 hodin tolik pozornosti, stále ještě probíhají. Zkušenosti z velmi podobných, starších případů, ukazují, že rychlé a jednoduché rady typu aktualizování operačních systémů, bezpečné chování na internetu a pod. nejsou pro organizace využitelné. Tyto a podobné rady rozdávají teoretici, kteří nebyli nikdy zodpovědní za provoz a zabezpečení rozsáhlých sítí korporací. Jedná se o sítě, které mají stovky serverů, pracovních stanic, aplikací a desítky tisíc zákazníků závislých na digitálních službách 24 hodin denně (např. internetové bankovnictví). Takové rady pouze napomáhají budovat falešný pocit bezpečí.

Včasná aktualizace operačního systému je nutnou, ne však postačující podmínkou. Nevyplácí se spoléhat jen na výrobce a dodavatele operačních systémů. Je zapotřebí investovat mnoho úsilí do správného návrhu a zabezpečení počítačové infrastruktury, monitorování bezpečnosti a v neposlední řadě také výcviku pracovníků, kteří jsou v organizaci odpovědní za bezpečnost. Ti musí vědět, jak se zachovat, když bude cílem jejich síť.

I když útočník prolomí všechna bezpečnostní opatření, musí být schopni prolomení odhalit dříve, než dojde k vážným škodám, případně tyto škody co nejvíce omezit. Musí vědět, jak zabránit dalšímu šíření nákazy a v neposlední řadě se pokusit o záchranu a obnovu zašifrovaných dat na disku.

Lukáš Kypus
CyberGym Europe, a.s.