E-Bezpečí 2020, 5(2): Page 29-30. Univerzita Palackého v Olomouci. ISSN 2571-1679.
Online: https://www.e-bezpeci.cz/index.php?view=article&id=2008

ČTVRTINA SPRÁVCŮ POČÍTAČOVÝCH SÍTÍ ČESKÝCH ŠKOL POTVRDILA, ŽE JEJICH ŠKOLA ZAŽILA ÚTOK NA POČÍTAČOVOU SÍŤ. PŘEVAŽUJÍ ÚTOKY SPOJENÉ S RANSOMWARE.

Kamil KOPECKÝ

Potvrzuje to nový český výzkum Český učitel ve světě technologií, který zrealizovala Univerzita Palackého v Olomouci ve spolupráci se společností O2 Czech Republic. Do výzkumu se zapojilo přes 2000 učitelů z celé České republiky - včetně správců školních počítačových sítí.

95,6 % správců školní počítačové sítě potvrdilo, že jejich škola využívá aktivní firewall (v aktivním síťovém prvku apod.), 93 % škol má také aktivní školní WiFi. Ta je zabezpečena nejčastěji pomocí protokolu WPA2 (45,36 %), filtrací MAC adres (19,44 %) či autentizací klienta (18,79 %).

Téměř čtvrtina oslovenských správců počítačových sítí škol (23,29 %) potvrdila, že jejich škola zažila útok na počítačovou síť.

Nejčastěji se školy potýkají s tzv. *ransomwarem*, který se do sítí dostává především prostřednictvím e-mailových účtů - a to zpravidla prostřednictvím infikovaných příloh, které nepozorný učitel otevře (v několika případech otevřel infikovanou přílohu sám ředitel školy). Po infikování klientského počítače se pak ransomware může rozšířit do dalších počítačů, potažmo celé počítačové sítě.

U incidentů spojených s ransomware dochází zpravidla k zašifrování dat školy a požadování “výkupného” za jejich rozšifrování a uvedení sítě do původního stavu. Školám pak nezbývá než obnovit veškerá data ze záloh. V řadě případů však škola o svá data přišla, protože neměla jejich zálohy a nebyla schopna (a ani nechtěla) uhradit vysoké výkupné.

Dalším častým typem útoků reportovaným učiteli jsou tzv. DDOS útoky, obecně také malware apod. Průniky přes krádeže hesel (či přímo jejich uhodnutí) jsou spíše raritní. Přesto školy reportují také pravidelné snahy o odhalení hesel pro vstup k Bakalářům a na vzdálenou plochu pomocí brute-force hádání hesel.

Pro E-Bezpečí
Kamil Kopecký