Vážené čtenářky, vážení čtenáři,

není to tak dlouho, kdy se obětí hackerů stala benešovská nemocnice. Velké manévry příslušných úřadů dávaly tušit, že jde o zásadní problém pro společnost, a tudíž že se z toho vyvodí i patřičné závěry. A jaký je výsledek? Před pár dny došlo k dalšímu útoku na nemocniční zařízení, tentokrát na daleko větší Fakultní nemocnici v Brně.

Podle prvních závěrů šlo opět o stejný scénář – prostřednictvím nakažené zprávy elektronické pošty došlo k aktivaci vyděračského ransomwaru, který zašifroval některá důležitá data nemocnice, a tím pádem ji znepřístupnil pro pacienty.

I když následky nebyly tak velké jako v prvním případě, protože řada oddělení zůstala otevřená především díky tomu, že její systémy nebyly připojené k centrální síti nemocnice, ukázalo se v plné nahotě, že zdravotnictví, tento nadmíru regulovaný obor, má velké nedostatky v zabezpečení svých systémů.

Ransomwarové útoky proti nemocnicím ale nejsou žádnou vzácností ani ve světě. Známé jsou případy z USA, Velké Británie, Německa či Rumunska. Ze statistik společnosti Kaspersky vyplývá, že v roce 2017 se ransomwarem infikovalo 30 % počítačů a zařízení využívaných ve zdravotnických organizacích. V roce 2018 jejich počet klesl na 28 % a vloni to bylo 19 %.

Pro tyto útoky přitom existují dva hlavní důvody: nedostatek pozornosti věnované rizikům spojeným s digitalizací a nedostatečné povědomí o kybernetické bezpečnosti ze strany zaměstnanců, neboť velká část pracovníků nikdy neprošla školením zaměřeným na kybernetickou bezpečnost.

Často se lze podle expertů setkat se situacemi, kdy na některých systémech neběží antivirus nebo je operační systém zastaralý (výjimkou nejsou ani PC se starými Windows XP), hesla používaná správci a uživateli jsou slabá a uživatelé otevírají soubory přiložené k e-mailům, aniž si ověřují jejich zdroj.

Výsledkem napadení pak také často bývá, že organizace volí raději zaplatit výkupné, než aby prošly martyriem všech těch kroků, které jsou s obnovou dat a systémů spojené, což samozřejmě činí z tohoto oboru ještě atraktivnější cíl. Problém ransomwaru je samozřejmě širší, ale právě u nemocnic je asi nejkřiklavější.

A co dělat, abyste se tomu vyhnuli? Deloitte radí udržovat kritická data rozčleněná, takže je pro ransomware těžší je zašifrovat, zakázat spuštění externích služeb na připojených zařízeních, zavést zásady, které zakazují na kritickém hardwaru přistupovat k osobnímu e-mailu nebo hraní her.

Osvědčilo se také velkou pozornost věnovat zálohovacím řešením, vyškolení všech zaměstnanců, aby si více uvědomovali kybernetickou bezpečnost, a čas od času použít různá cvičení pro simulaci útoků pomocí ransomwaru, třeba formou nějaké hry.

A samozřejmostí je pravidelná oprava a aktualizace systémů i softwaru a také sdílení informací či poučení se z úspěchů a selhání druhých.

S přáním, abyste ve zdraví přežili současné komplikace a úspěšně restartovali své podnikání – to se díky tomu, že se ukázalo, že mnoho pracovních pozic lze převést na distanční nebo digitalizovanou formu, totiž může brzo zásadně změnit…

Pavel Louda
vedoucí projektu

Obsah