Niekedy intenzívne útoky DDoS trvajú aj niekoľko týždňov. Pri takýchto útokoch je ideálne mať za sebou silného a odborne zdatného IT partnera, ktorý dokáže svojimi skúsenosťami a s tímom odborníkov poskytnúť pohotovo technickú a organizačnú pomoc, čo môže zabrániť vážnym škodám hroziacim spoločnosti.

NXT A ako je to s drahocennými dátami firiem? Vieme, že firemné údaje sú najcennejšie vlastníctvo firiem, ako ich teda čo najlepšie ochrániť? Nestačí vlastný server...?

Roman Vavrík: Vlastné dáta sú najcennejšie hodnoty každej spoločnosti, ktoré si zaslúžia pozornosť. Opäť platí pravidlo, že firmy môžu mať vlastné servery, kde prevádzkujú a, samozrejme, aj ochraňujú a pravidelne zálohujú svoje údaje. Na tom v podstate nie je nič zlé, problém nastane až vtedy, keď príde k nežiaducej katastrofe, ako je napr. skrat v serverovni, preťaženie alebo výpadok napájania, alebo ak nejaká prírodná katastrofa alebo poveternostné vplyvy zasiahnu a spôsobia škody bez možnosti jednoduchej nápravy. V tomto prípade je lepšie siahnuť po využití profesionálne poskytovaných cloudových službách, pri ktorých odpadajú mnohé zo spomenutých rizík, pretože na všetko dohliada tím odborníkov v prevádzkovom režime 24×7 počas celého roka. Dáta sú bezpečne uložené v dátovom centre, do ktorého nemá nik iný prístup okrem poverených pracovníkov spoločnosti, ktorá si zriadila takýto typ služieb.

Ak sa vrátime k aktuálnej pandemickej situácii a práci z domu, ďalší z benefitov je napr. len obyčajné zdieľanie veľkoobjemových dát. Dosť často sa stáva, že pri niektorých povolaniach firemní zamestnanci pracujú s veľkokapacitnými dátami, ktoré si medzi sebou vymieňajú či pripomienkujú. Pri práci z domu je niekedy obťažnejšie ukladať či zdieľať takéto dáta a poväčšine zamestnanci hľadajú voľne dostupné public riešenia na uschovanie či posielanie takýchto dát, čo môže vážne ohroziť nielen dáta spoločnosti, ale aj jej riadny chod, pretože tak vystavujeme cenné data nebezpečenstvu možného zneužitia. Pri spracovaní a príprave takýchto dát by s istotou pomohlo cloudové riešenie od vlastného zamestnávateľa. Tak si obe strany môžu byť isté, že nepríde k ohrozeniu spracovávaných dát a ani k ich sprístupneniu nepovolaným osobám.

NXT: Vyzerá to tak, že pandémia nás ešte nejakú tu chvíľku potrápi. Máte nejaký návod na to, ako zvládnuť prácu z domu? Na čo by si mali zamestnávatelia, ale hlavne zamestnanci dávať pozor, aby neohrozili seba a svoju spoločnosť?

Roman Vavrík: Základ je, aby sme všetci ostali zdraví. V dnešnej dobe je ľudské zdravie najcennejšie, preto by zamestnávatelia mali myslieť na svojich zamestnancov a v čo najväčšej miere im umožniť prácu z domu, pokiaľ to charakter ich práce dovoľuje. Firmy by však súčasne mali myslieť na to, ako čo najlepšie zabezpečiť svoje podnikové aplikácie a systémy na diaľku tak, aby ich zbytočne nevystavovali hrozbe.

Zároveň aj zamestnanci by mali mať na pamäti, že svoj pracovný nástroj v podobe notebooku či stolového počítača by mali využívať hlavne na prácu, a pokiaľ majú možnosť, pripájať sa cez VPN, mať neustále aktualizovaný kancelársky a používateľský softvér, rovnako aj antivírusové programy a VPN klienty a neotvárať žiadne podozrivé maily, nesťahovať prílohy od neznámych adresátov či neinštalovať nepracovné programy do svojich firemných zariadení. Všetky vymenované zásady znižujú možnosti na kybernetické útoky a ohrozenia. ■

AKO POSILNIŤ KYBERBEZPEČNOSŤ FIRMY, ABY AJ PRÁCA Z HOME OFFICE BOLA BEZPEČNÁ

Pri práci z domu je najdôležitejšie, aby používateľ mohol vzdialene a hlavne bezpečne pristupovať (napr. pomocou VPN) do firemnej infraštruktúry, do interných systémov. V čase, keď sme ešte chodili do kancelárií, vzdialený prístup sa využíval v omnoho menšej miere a záťaž na firemnú konektivitu nebola až taká vysoká. Aktuálnou situáciou sa podmienky zmenili a bolo treba vyriešiť optimalizáciu vzdialeného prístupu tak, aby bol stabilný a zvládol nápor všetkých pripojených zamestnancov pracujúcich z domu a aby zároveň bola zachovaná vysoká miera bezpečnosti. Ideálny kompromis je vyňať z VPN prístup do internetu a komunikačných služieb, ktoré sa využívajú najmä pri online komunikácii a stretnutiach, ako sú Teams, Zoom, Webex. Tieto aplikácie sú náročnejšie na záťaž linky. Tým docielime optimalizáciu prístupu k interným systémom firmy cez VPN a zároveň zachováme pohodlnú komunikáciu počas online stretnutí, ako aj vysokú mieru zabezpečenia či už z pohľadu vzdialeného prístupu, alebo využitia komunikačných nástrojov.

Takisto netreba zabúdať ani na zabezpečenie e-mailovej komunikácie. Pomocou rôznych bezpečnostných nástrojov možno efektívne detegovať spam a phishingovú poštu, ktorá predstavuje pre spoločnosť a zamestnancov potenciálne bezpečnostné riziko. Toto riziko tiež môžeme eliminovať pravidelným školením zamestnancov vo forme online prezentácií, školení alebo posielania pravidelných newsletters o bezpečnostnom povedomí (Security Awareness Training).

Dôležité je takisto dbať na bezpečnosť všetkých firemných systémov, aby boli pravidelne aktualizované, dostatočne zabezpečené a využívali len silné šifrovacie protokoly pri komunikácii. Netreba zabúdať ani na bezpečnosť počítačov zamestnancov, ktorí pracujú z domu, aby mali nainštalované pravidelné aktualizácie systému a aktívnu antivírusovú ochranu.

Situácia počas pandémie paradoxne urýchlila a nastavila trend migrácie firemných riešení do cloudového prostredia, vďaka čomu firma získa oveľa väčšiu flexibilitu služieb a aj škálovateľnosť v porovnaní s tradičnými serverovými riešeniami. Veľký benefit je podpora rôznych platforiem, ako sú mobilné zariadenia, tablety a počítače s rôznymi operačnými systémami. Takisto pri cloudových službách sa kladie veľký dôraz na bezpečnosť. Dobrý príklad je viacfaktorová autentifikácia používateľov alebo definovanie bezpečnostných politík organizáciou, ako k jednotlivým službám pristupovať a publikovať ich.

» FILIP **MIKUŠ**
SECURITY TEAM LEAD ALITER TECHNOLOGIES