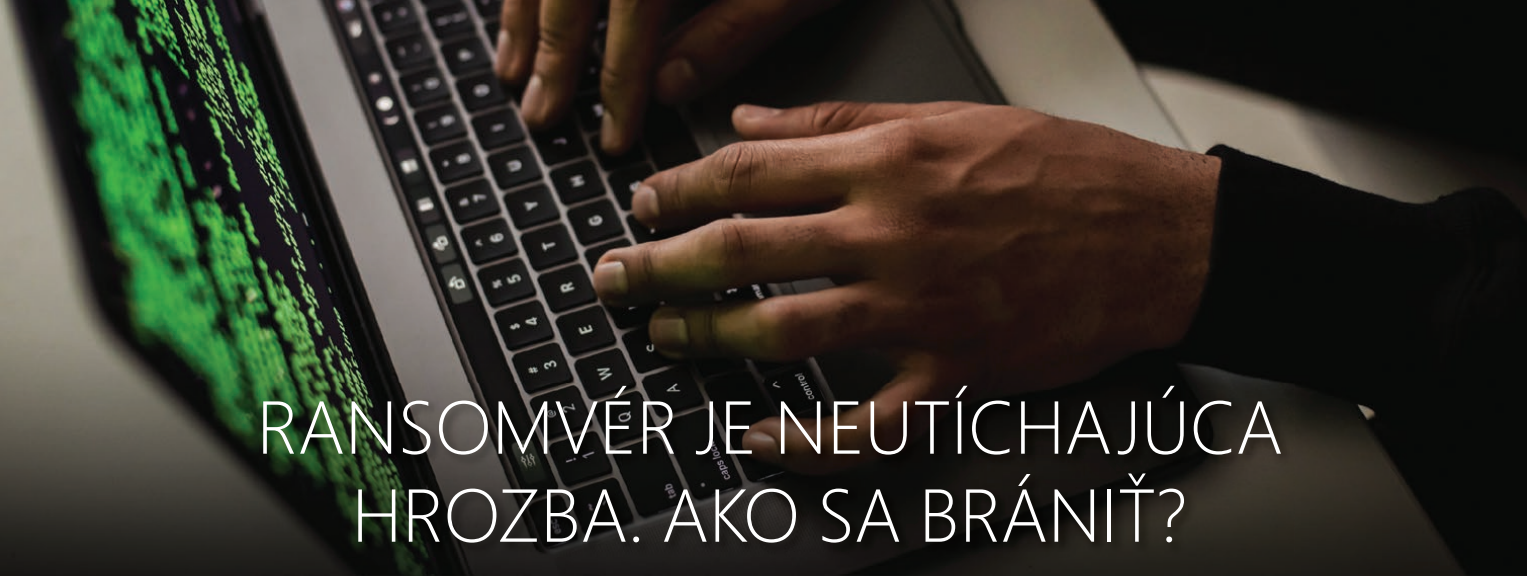
NEXTECH

KYBERNETICKÁ BEZPEČNOSŤ PRE FIRMY

PREVENCIA
Ako sa pripraviť a priebežne kontrolovať stav ochrany

OCHRANA
Aké útoky hrozia firmám a ako sa pred nimi chrániť

REAKCIA
Čo robiť ak už k útoku došlo, ako reagovať



RANSOMVÉR JE NEUTÍCHAJÚCA HROZBA. AKO SA BRÁNIŤ?

Ransomvér je typ škodlivého softvéru (malware – malicious software), ktorý po napadnutí počítačového systému zabráni používateľovi pristupovať k dátam tým, že ich zašifruje. Doterajšia prax útočníkov spočívala zväčša v požiadavke na zaplatenie finančnej sumy za navrátenie tohto prístupu. Takéto útoky môžu spôsobiť značné škody prerušením firemných procesov a viesť aj k trvalej strate dát.

Za posledné dva roky možno sledovať značný nárast počtu ransomvérových útokov. Podľa údajov Temple University* sa zvýšil počet nahlásených ransomvérových útokov na kritickú infraštruktúru medzi rokmi 2018 a 2019 takmer trojnásobne a medzi rokmi 2019 a 2020 skoro dvojnásobne. V roku 2021 bolo do polovice mája nahlásených 97 ransomvérových útokov na kritickú infraštruktúru.

Vo všeobecnosti sme doposiaľ vídali dve kategórie ransomvérových útokov:

1. kategória – útočník zašifruje pevné disky a žiada výkupné za sprístupnenie dát
2. kategória – útočník zašifruje súbory a žiada výkupné za poskytnutie dešifrovacieho kľúča

V poslednom čase sa začína viac a viac objavovať tretia kategória ransomvérových útokov, keď útočník ukradne veľké množstvo dát a potom hrozí ich zverejnením, ak mu nezaplatia výkupné. Jeden z dôvodov, prečo to tak je, tkvie v skutočnosti, že sa objavujú nové nástroje, ktoré sa zameriavajú na útoky prvej a druhej kategórie a vedia ich blokovať. Napríklad Microsoft má nástroje schopné monitorovať adresáre a detegovať a následne zablokovať neautorizované procesy (aplikácie), napríklad šifrovanie. Alebo môžeme použiť nástroj s názvom Raccine, ktorý vie úspešne zabrániť ransomvéru, ktorý zneužíva vssadmin.exe, aby zmazal „tieňové" kópie (shadow copies) uložené na napadnutom počítači, a potom zablokuje proces, ktorý túto požiadavku spustil. Takisto pravidelné zálohovanie s testovaním záloh a ich bezpečné uloženie dopomáha k zmenšovaniu dôsledkov na firemné procesy súvisiace s týmito kategóriami ransomvérových útokov.

Tretia kategória ransomvérových útokov sa postupne stáva dominantnou a je pravdepodobné, že to takto ešte nejaký čas aj zostane. Prečo to tak je? Ako sme už spomenuli, nové nástroje robia ransomvérové útoky prvej a druhej kategórie čoraz zložitejšími. Preto skupiny, ktoré sa zaoberajú takouto protiprávnou

** Rege, A. (2021). "Critical Infrastructure Ransomware Incident Dataset". Version 11. Temple University. Online at https://sites.temple.edu/care/resources/. Funded by National Science Foundation CAREER Award #1453040*

aktivitou, smerujú svoje úsilie do oblasti, kde z pohľadu ich „obchodného modelu" majú vyššiu šancu na zisk. Ak útočník použije taktiky a techniky, ktoré udržia jeho profil pod úrovňou detekcie v napadnutom systéme, možno predpokladať, že sa bude pohybovať v napadnutom systéme dlhodobo (podľa SANS 2019 Incident Response Survey je v prípade 42 % organizácií čas potrebný na odhalenie útočníka v napadnutom systéme v rozsahu dní až mesiacov; podľa špeciálnej správy M-Trends 2021 je globálny medián času potrebného na odhalenie útočníka v systéme 24 dní) a zhromažďovať veľké objemy firemných dát bez toho, aby sme o tom vedeli.

Tu sa do popredia dostáva aktívne vyhľadávanie hrozieb v počítačovej infraštruktúre. Perspektívna a vysoko účinná technika je vytváranie falošných nastražených dokumentov – honeydocs, ktoré sú zaujímavé z hľadiska potenciálneho útočníka. Napríklad môže ísť o súbor .xlsx s podstrčeným zoznamom hesiel. Rovnako zaujímavé z pohľadu útočníka sú aj nastražené administrátorské účty, tzv. honeyaccounts. Obe metódy sú v prípade neoprávnenej manipulácie alebo použitia schopné poslať hlásenie v reálnom čase a upriamiť tak pozornosť SOC (Security Operation Center) operátora a vzápätí iniciovať reakciu na danú udalosť. Túto stratégiu možno implementovať za veľmi krátke obdobie a takisto s rozumným rozpočtom.

Ďalšia perspektívna stratégia aktívneho odhaľovania útočníka v sieti je inšpekcia/monitoring komunikácie so vzdialeným riadiacim počítačom (command and control alebo C2) – v angličtine sa tento druh komunikácie označuje beacon. Samozrejme, tento druh komunikácie používajú aj legitímne a autorizované aplikácie, preto je dôležité vedieť, na čo sa zamerať. Tento prístup vyžaduje, aby sme sa nepozerali na individuálne relácie TCP, ale na komunikáciu ako celok z pohľadu väčšieho časového úseku. Toto nám pomôže identifikovať anomálie, ktoré vedú k odhaleniu neautorizovanej komunikácie. Na podporu tejto stratégie existuje bezplatný nastroj RITA (Real Intelligence Threat Analytics), ktorý v súčasnosti okrem detekcie C2 komunikácie využíva aj ďalšie možnosti kontroly.

Do budúcnosti sa dá predpokladať jednoznačne stúpajúci trend ransomvérových útokov tretej kategórie a tomuto trendu treba prispôsobiť aj obranné stratégie počítačovej infraštruktúry.

DANIEL SUCHÝ, špecialista na kybernetickú bezpečnosť,
Aliter Technologies, a. s.

ZERO TRUST

Zero trust nie je nič nové. Tento koncept bol predstavený už v roku 2010 a jeho hlavné zameranie je ochrana dát. Odvtedy uplynulo už viac ako 10 rokov, ale rozsiahlejšie implementácie bolo možné zaznamenať až minulý rok, keď museli malé firmy aj veľké korporácie prejsť z práce v kanceláriách (konvenčný model) na prácu z domu pri veľkej väčšine zamestnancov. Ten, kto by si myslel, že ide o niečo jednoduché, sa mýli. Rovnako ako ten, kto by si myslel, že zaobstaraním a implementáciou novej technológie, ktorá je hrdo označená zero trust, je úloha splnená. Štandardne sa takýto proces plánuje na dva a viac rokov. No minulý rok priniesol aj naozajstné výnimky, keď niektoré spoločnosti implementovali architektúru zero trust takpovediac cez noc. Čo je teda zero trust?

V skratke možno zero trust vyjadriť ako „ničomu nedôveruj a všetko preveruj". Neexistuje jednotná definícia, no vo všeobecnosti sa dá povedať, že zero trust je neustále sa vyvíjajúca stratégia kybernetickej bezpečnosti s cieľom opustiť zastaraný konvenčný statický model, založený na ochrane perimetra, a zamerať sa na dynamickejší prístup cez používateľov, zariadenia a zdroje.

Konvenčný model má viac-menej dve kritériá. Všetko, čo je mimo firemnej siete (internet), pokladá za nedôveryhodné a všetko v rámci firemnej siete (LAN) za dôveryhodné. Rovnaký prístup je aj na základe vlastníctva zariadenia – firemné je dôveryhodné, súkromné zariadenie je nedôveryhodné. Toto však už dávno neplatí.

Architektúra zero trust je iba odpoveď na trendy v rámci firemnej (korporátnej) infraštruktúry vrátane vzdialeného prístupu (napr. práca z domu), používania súkromných zariadení na pracovné účely (BYOD) a, samozrejme, firemných aktív umiestnených v cloude. Môžeme povedať, že ani v jednom z týchto prípadov nemáme kontrolu nad tým, kde sa takéto aktívum nachádza. S určitosťou však vieme, že nie je v uzavretej firemnej sieti (v konvenčnom ponímaní) s pevne definovanými hranicami. Preto sa stratégia zero trust zameriava

na ochranu zdrojov (firemné aktíva, služby, sieťové účty, workflow atď.), a nie na sieťové segmenty, pretože lokalita v sieti už nie je primárnym komponentom bezpečnostného statusu zdroja. Stratégia zero trust sa líši od konvenčného prístupu tým, že automaticky nepovažuje používateľov a zariadenia za dôveryhodné iba na základe fyzickej polohy alebo „polohy" v sieti, resp. vlastníctva zariadenia.

Zhrňme si teda základné princípy architektúry zero trust:

1. Vždy pristupujte k vašej internej/externej sieti, akoby bola napadnutá
2. To, že je sieť interná, nie je dostatočný argument na to, aby sme jej dôverovali
3. Každé zariadenie, používateľ a komunikácia v sieti musia byť preukázateľné
4. Nepretržitý hĺbkový monitoring siete

Nepretržitý monitoring siete je základný prvok, ktorý umožňuje identifikáciu a klasifikáciu dát, mapovanie pohybu citlivých dát, porozumenie vlastnej sieti, zariadeniam a aplikáciám. Je potrebné, aby riešenie na monitorovanie siete bolo nepretržité a jeho nastavenie umožňovalo aj monitorovanie komunikácie v rámci internej siete, medzi internými zariadeniami. Následne je ideálne prepojenie na SIEM (nástroj na monitorovanie a odhaľovanie kybernetických hrozieb). Ten zhromažďuje záznamy, ktoré nás zaujímajú, a pomáha zachytiť potenciálnu prítomnosť útočníka/hrozby v sieti. Takisto vie vykonať preddefinovanú akciu na základe nastavených algoritmov.

A ako začať? Ak používate hlavne prostredie Windows, na to, aby ste začali uplatňovať stratégiu zero trust, pravdepodobne nepotrebujete nič extra okrem toho, čo už máte vo svojej infraštruktúre. Napríklad namiesto jednostrannej autentifikácie zo strany servera začnite uplatňovať vzájomnú autentifikáciu na komunikáciu medzi serverom a klientom s využitím internej PKI (Public Key Infrastructure – systém na tvorbu a distribúciu digitálnych certifikátov). Druhým príkladom môže byť izolácia domén a vynútenie IPsec (Internet Protocol security – autentifikačný a šifrovací protokol) atď.

Pre tých, ktorí by sa chceli dozvedieť viac o koncepte zero trust, odporúčam knihu *Zero Trust Networks: Building Secure Systems in Untrusted Networks* od Evana Gilmana a Douga Bartha.

DANIEL SUCHÝ,
špecialista na kybernetickú bezpečnosť, Aliter Technologies, a. s.