Tlačová správa

Bratislava 25. september 2023

Sme pripravení na kybernetické hrozby?

V súčasnosti sme svedkami zvýšeného počtu útokov na univerzity, kedy útočníci žiadajú výkupné. Tieto aktivity hackerských skupín nám jasne ukazujú, že je potrebné venovať väčšiu pozornosť kybernetickej bezpečnosti. Čo to vlastne znamená?

- Ransomvérový útok je druh kybernetického útoku, pri ktorom útočníci infikujú cieľový počítačový systém škodlivým softvérom nazývaným ransomvér (tiež ransomware). Tento škodlivý program zablokuje prístup k dôležitým súborom alebo k celému počítačovému systému tým, že tieto údaje zašifruje. Útočníci potom žiadajú od svojej obete výkupné (ransom), aby získala kľúč na odšifrovanie týchto údajov. Obeť je vydieraná a musí zaplatiť požadovanú sumu, aby získala späť kontrolu nad svojimi dátami alebo systémom, ktorý bol počas útoku uzamknutý.

Ransomvérové útoky môžu postihnúť jednotlivcov, firmy, školy, ale aj verejné inštitúcie. Útočníci často požadujú výkupné v kryptomene (napríklad Bitcoin) a hrozia, že ak nebude výkupné zaplatené, dáta budú trvalo stratené alebo zverejnené. Tieto útoky sa môžu šíriť prostredníctvom infikovaných e-mailových príloh, škodlivých odkazov alebo zneužitím bezpečnostných slabín v softvéri. Zásadná je správna bezpečnostná stratégia pre ochranu dát a systémov.

Kybernetická bezpečnosť funguje pre náš digitálny svet ako ochranný štít. Ransomvérové útoky sú podobné digitálnym únoscom, ktorí zašifrujú naše dôležité súbory až do chvíle, kým im nezaplatíme výkupné. Aké sú najčastejšie vstupné brány? Predstavte si, že vaša sieť je ako dvere do vášho domu. Ak nie sú dvere zabezpečené, teda uzamknuté alebo dokonca široko otvorené, zlodeji sa môžu ľahko dostať dnu. Podobne sa aj nesprávne nakonfigurované služby a otvorené porty v sieti môžu stať ľahkým cieľom pre útočníkov.

Ďalšou slabinou je, že organizácie často nemajú dostatočný prehľad o tom, aké systémy vlastnia a používajú. Chýba im systematický spôsob ako evidovať a udržiavať záznamy o počítačoch, serveroch, softvéroch alebo iných digitálnych zariadeniach a prostriedkoch, ktoré sú v ich vlastníctve a sú využívané v sieti. Je to trochu ako mať v dome veci, o ktorých ani nevieme, pretože nikdy neboli nikde zaznamenané. Je logické, že firma len ťažko ochráni server alebo informačný systém, o ktorom netuší, že ním disponuje.

Na Fakulte informatiky a informačných technológií STU v Bratislave sa aktívne zaoberáme otázkami týkajúcimi sa bezpečnosti a súkromia v rámci našej výskumnej skupiny Cyber Security and IoT. Zameriavame sa na oblasti, akými sú bezpečnosť smerovania údajov medzi internetovými poskytovateľmi (protokol BGP – Border Gateway Protocol), ochrana bezdrôtových sietí vrátane technológií ako WiFi a Bluetooth a tiež na technológie pre Internet vecí vrátane LoRa a iných protokolov.

Náš hlavný cieľ spočíva v tom, ako systematicky zabezpečiť infraštruktúru informačných technológií. Aktívne vyhľadávame potenciálne slabiny a nezrovnalosti pomocou modelov strojového učenia, ktoré

Ilkovičova 2
842 16 Bratislava
Slovensko
www.stuba.sk

media@fiit.stuba.sk
T: +421 908 978 947

mnohí poznajú pod pojmom "umelá inteligencia" (AI). Taktiež budujeme monitorovací systém pre siete a koncové zariadenia, čo je kľúčovým prvkom aktívnej prevencie a rýchlej reakcie v oblasti bezpečnosti.

„*Vzhľadom na rastúci počet elektronických informácií a služieb sa zvyšuje aj hodnota týchto aktív. To znamená, že sú čoraz častejším cieľom útokov. Hoci sa investuje veľa zdrojov do rôznych bezpečnostných systémov, tieto systémy slúžia skôr ako podpora pre odborníkov na kybernetickú bezpečnosť, nie ako ich plnohodnotná náhrada. Je dôležité, aby odborníci vedeli efektívne využiť tieto nástroje a metódy na zlepšenie bezpečnosti IT a komunikačných systémov. Praktické skúsenosti s týmito nástrojmi môžu nadobudnúť napríklad cez realistické hry v kybernetickom polygóne Cyber Range*," uviedol vedúci výskumnej skupiny Cyber Security and IOT(CSI) Pavol Helebrandt, ktorý pôsobí na FIIT STU ako odborný asistent.

V rámci platformy Cyber Range možno simulovať rôzne situácie a útoky, ktorým sú počítačové siete, systémy a aplikácie vystavené. Účastníci Cyber Range sa tak môžu učiť, ako reagovať na reálne hrozby, rozpoznávať bezpečnostné slabiny a aplikovať bezpečnostné opatrenia bez toho, aby to ovplyvnilo skutočné prostredie. Ide o užitočný nástroj na zdokonalenie praktických zručností a schopností v oblasti kybernetickej bezpečnosti.

Ako dodáva člen výskumnej skupiny Cyber Security and IOT Alexander Valach, ktorý je doktorandom na FIIT STU: „*Žiadnu z týchto oblastí by sme nemohli skúmať bez potrebného tréningu a vzdelávania v oblasti kybernetickej bezpečnosti prostredníctvom projektov FIIT Academy a Sieťovej akadémie na FIIT STU v rámci Centra ďalšieho vzdelávania.“*

Na Fakulte informatiky a informačných technológií STU v Bratislave sa snažíme posilňovať bezpečnosť digitálneho sveta pred narastajúcimi hrozbami kybernetických útokov. Investície do kybernetickej ochrany sú absolútnou nevyhnutnosťou, pretože tieto hrozby sú čoraz sofistikovanejšie.