KYBERNETICKÝ ÚTOK

Kybernetické útoky jsou nebezpečné a v poslední době časté. Kybernetický útok je útok hackerů v kybernetickém prostoru na různých místech. Například nemocnice, ty by měly být chráněné a měly by umět útoky odrážet. Jinak by po útoku mohly přijít například o některá administrativní a ekonomická data nebo o internetový objednávkový systém u dárců krve. Hackeři se díky tomu dostanou k osobním informacím pacientů a dárců. Dozví se jejich data narození, místo bydliště, jakou mají zdravotní pojišťovnu a tak dále. Takový případ se stal například v České republice v Brně třináctého března 2020. Kdyby se hackeři dostali do serveru elektronického receptu, mohli by zjistit, kdo užívá jaké léky a mohli by tyto informace prodávat firmám a ty by například nabízeli svoje produkty.

Silně chráněny před kybernetickými útoky by měly být také pojišťovny a banky. Dnes už se mnoho lidí pojišťuje nebo si zakládá své účty přes internet. Při pojištění na internetu musíte zadat spoustu svých osobních údajů, které se dají lehce zneužít a prodávat firmám. Při kybernetickém útoku na banky by hackeři mohli získat citlivé informace. U lidí, kteří používají internetové bankovnictví by se dokonce mohli dostat na jejich účet a platit přes něj. Hackeři se mohou pokusit dostat do serveru jakékoliv firmy a potom už jen záleží na tom, jak silnou má firma ochranu. Když se hackeři přes kyberprostor dostanou na server dané společnosti, můžou najít kolik ve firmě protéká peněz, nebo kdo jsou její zákazníci. Tyto informace můžou poskytnout konkurenční firmě a napadená firma může zkrachovat. Může se stát, že se hackeři dostanou do serveru pracovního mailu a vydávají se za některého zaměstnance. Mohou tak z finančního oddělení podvodným způsobem vylákat nemalé množství peněz na své účty. Další varianta je, že zneužijí nepozornosti zaměstnanců. Na první pohled zaslaný mail například od nadřízeného,

který se také může týkat převodu peněz na určitý účet nebo proplacení faktury, vypadá stejně jako by ho nadřízený sám zaslal. Tak zvaný nickname je jméno nadřízeného, ale když nickname rozklikneme, tak vidíme, že je pod ním schovaný jiný emailový účet než od nadřízeného. Když je ovšem zaměstnanec nepozorný, pošle peníze na účet, který byl napsán v mailu. Že to byl podvod, se zjistí až později, nebo se to, že je to podvod nemusí zjistit vůbec. Případů, kdy se to zjistilo, ale už se to nedalo zachránit, je mnoho po celém světě, ale i v České republice.

Jeden ze způsobů, jak hackeři útočí na firmy je použití malwaru. Malware je škodlivý program, který se pokouší proniknout do slabých míst aplikací a programů a dostat se k citlivým informacím. Známým případem v Čechách je, že stále hodně počítačů používá operační systém Windows 7, na který již Microsoft nevydává aktualizace. Tím pádem jejich uživatelé nejsou ochráněny před nejnovějšími hrozbami a mohou v něm vzniknout zadní vrátka pro proniknutí škodlivých malwarů.

Hackeři se mohou dostat i do dat z bezpečnostních kamer. Následně si můžou data stáhnout a popřípadě vydírat osoby zachycené na kameře,. nebo zjistit v kolik hodin chodí na určité místo a potom člověka přepadnout.

Hacker by přes sociální sítě pomocí kybernetického útoku mohl vydírat a poškozovat kohokoliv, kdo sociální sítě používá nebo je někdy navštívil. Častým cílem jsou známé osobnosti, například herci, zpěváci, influenceři, nebo politici.

Pomocí kybernetického útoku by hacker mohl také zaútočit na různé aplikace. Velký problém by mohl být u těch aplikací, kterým jste povolili zjišťování vaší polohy, přístup k souborům nebo fotoaparátu. Proto byste si měli dávat velký pozor na to, jak jsou aplikace, které jste povolili- zjišťování vaší polohy, přístup k souborům a fotoaparátu, bezpečná.

Všichni hackeři nemusí útočit se špatným záměrem. Některé kybernetické útoky si dokonce platí samy firmy, za účelem zjištění, jak je jejich ochrana antivirusy silná a účinná. Těmto hackerům, kteří pomáhají firmám, se říká modré klobouky.

Někdy hackeři se mohou pokusit ovlivnit veřejné mínění, nebo dokonce volby v cizím státě. Poslední dobou jsou diskutovány aktivity hackerů pro tajné služby. Vytvářejí např. tisíce uživatelských účtů na rozličných sociálních sítí, kde pomocí „fakenews“ a jiných zmanipulovaných informací, snaží ovlivnit veřejné mínění určitým směrem. Nejvíce mediálně známé jsou činnosti ruských a čínských tajných služeb.

Hackeři můžou dokonce započít válku. Pokud chce nějaká země (třetí země) z například politických důvodů, aby jiné dvě země proti sobě válčily, tak si třetí země najme hackery. Tito najatí hackeři mají za úkol dostat se do armádního serveru první země. Když se jim podaří do tohoto serveru dostat, můžou teoreticky zahájit útok, nebo i odpálit atomovou bombu z první země do druhé země. Tímto závažným krokem můžou i spustit válku. Tento krok by mohl změnit mnoho životů, někteří lidé mohou přijít o svá obydlí, někteří mohou mít závažná zranění a někteří mohou dokonce ztratit i životy. Vzhledem k tomu, že by to byl závažný zločin, který by mohl ovlivnit dějiny lidstva, je nutné nebrat tato nebezpečí na lehkou váhu i za cenu vynaložení velkých finančních prostředků.

Myslím si že kybernetický útok by byl horší než pandemie Covid19, pokud by ohrožoval více životů než Covid19.