CYBER COVID ESEJ

Moderní svět je řížen něčím, co není vidět, ale přesto existuje. Každým dnem se setkáváme se spousty komplikovaných počítačových systémů, které nám umožňují žít takový život, který máme. Ráno vstaneme, budíkem nás vzbudí náš chytrý telefon. Rozsvítíme světla, elektřinu nám mile poskytnou distribuční systémy a energetické závody řízené SCADA systémy. Nasedneme do auta, a ještě před otočením klíčku již řídící jednotka vozidla obstarává vše potřebné pro běh motoru a řízení vozu. Na semaforech dostaneme zelenou od semaforu, který je už také často řízen centrálně. V práci si kontrolu nad našima odpracovanýma hodinama přejímá kontrolu firemní mzdový systém. A teď si představte, že každý z těchto systémů může být napaden.

Jak by vypadal takový den, kdyby někdo vyřadil z provozu energetickou síť obstarávající vaše město? Jak by to vypadalo, kdyby najednou na všech semaforech padla zelená? Co by jste dělali, kdyby se vaše auto najednou rozhodlo, že je vhodný čas zatočit mimo silnici do aleje stromů? Co by jste dělali, kdyby vám nepřišla dva měsíce výplata? A teď si představte, že se nebavíme o sci-fi, ale o dnešním dnu.

Doba postupuje, a čím více zařízení začíná přitahovat pozornost možnými bezpečnostními riziky. Čím více zařízení získává možnost se připojit k internetu. Nebude trvat dlouho, než i naše ledničky budou mít plnohodnotný operační systém. Možná už ji doma máte, ani o tom nevíte. Tomuto konceptu se říká Internet of Things. Neboli internet věcí, možnost různých běžných domácích zařízení spolu komunikovat, a nechávat se kontrolovat centrálním prvkem, třeba našim chytrým telefonem. Krásná představa, že vám kávovar uvaří kafe hned, jak mu telefon oznámí, že jste vzhůru, či po tom, co mu automobil oznámí, že parkujete u svého domu je zároveň nepěknou představou toho, že deset tisíc od výroby špatně zabezpečených kávovarů řízených jednou, nebo více osobami, které nad nimi převzali kontrolu provedou útok na výrobní závod ve vašem městě, a vy se ocitnete bez práce.

Některé společnosti také přemýšlí dopravovat zásilky domů drony, a tím výrazně zkrátit čas dopravy. Ale opět, pokud dojde kvůli špatnému zabezpečení k převzetí kontroly nad drony, a ty se rozhodnou, že spolu nalétají dopravnímu letadlu do motorů, nebo že je na čase nabrat rychlost 80km/h, a trasa letu vede po chodníku v úrovni hlavy chodců, tak již nám to nepřipadá jako dobrý nápad. S každým novým zařízením na internetu přibývají nová potenciální rizika, která je třeba vnímat.

Také se poslední dobou každým rokem vpřed vracíme zpět do Orwellového roku 1984. Nejsme avšak sledováni tolik státem, jako soukromými subjekty, které pak všechny naše osobní data prodají reklamním společnostem za pár dolarů.

Není to skvělé, jak nám Facebook říká, kdy mají naši přátelé narozeniny, co právě dělají, a kde jsou? Tak si v nastavení stáhněte svůj podrobný výpis, co vše je o Vás Facebooku známo, a budete velmi nemile překvapeni. Velmi často jsme dobrovolně profilováni do posledního detailu, jakým autem jezdíme, kde pracujeme, jaké jsou naše denní rutiny, s kým se bavíme, co si o čem myslíme, a tak dále. A to vše jen proto, aby nám vyskočila reklama na nové lyže zrovna v moment, kdy plánujeme výlet do hor. Aby nám vyskočila reklama na novou pračku ve chvíli, kdy již jsou se starou potíže. Kdyby nás někdo chtěl sledovat, ani nemusí přijet poblíž místa kde bydlíme. Jen na správných místech zaplatí, a ví o nás absolutně vše.

Jsou místa, kde se my můžeme bránit. Zabezpečit si všechny naše účty silnými hesly, používat dvoufázové ověření, kontrolovat si, zda jsme opravdu na té stránce, na které chceme být, nestahovat programy, které se jeví jako podezřelé, nesdílet zbytečně mnoho o sobě na sociálních sítích. Přesto, že toto slyšíme dnes a denně, stejně se tyto hrubé chyby opakují. Neberme toto na lehkou váhu.

Jsou ale pak místa, kde musíme spoléhat na ostatní, že svou práci odvedli dobře. Že si firmy své systémy dostatečně zabezpečili. Že město bralo v potaz možnost napadení při instalování nového chytrého systému řízení dopravy. Že výrobce automobilů počítal s tím, že vozidlo může být také cílem útoku. Že stát počítá s možností napadení. Že náše zákony chrání naše osobní data.

Právě z těchto důvodů existuje obor kybernetické bezpečnosti, kde se lidé učí jak najít slabiny systému, a jak ho pak zabezpečit. Jak vyzkoušet, zda je opravdu dané zařízení neprolomitelné. Zdali nějaký útok právě neprobíhá. A pokud již probíhá, jak minimalizovat škody. Tento obor bude zapotřebí nevyhnutelně každým dnem více, protože jak jsme si již řekli dříve, rizika stále přibývají, a dále přibývat budou.

Kybernetická kriminalita také neustále stoupá, již dnes je možné si „koupit“ osobu, která pak za úplatu provede jaký útok si přejeme, a je v jejích schopnostech. Představte si, že jedna firma zaplatí nemalou částku kriminálníkovi, aby dočasně vyřadil z provozu tržního protivníka, firmu ve které pracujete právě vy. A možnosti, jak zaútočit budou úměrně stoupat vůči počtu nových chytrých zařízeních právě v cílové firmě.

Druhá stránka věci jsou útoky politické, které se objevují, a budou čím dále tím častější. Narušováním infrastruktury znepřáteleného národu je možno dosáhnout velmi velkých škod s poměrně malými náklady, a mnohem menší mediální odezvou než kdyby stejného účinku chtěli dosáhnout konvenční metodou. Také je možnost se distancovat od samotného útoku pomocí sofistikovaného provedení. Je poměrně lehké vystopovat někoho, kdo sabotoval nemocnici zevnitř, než odhalit pachatele důmyslně provedeného kybernetického útoku na téže nemocnici.

Zranitelnosti budou tedy každým dnem přibývat, a my všichni bychom měli obor kybernetické bezpečnosti podporovat. Měli bychom si klást otázky, zdali jsou systémy, které používáme dostatečně zabezpečeny. Měli by jsme všichni stát za tím, aby se nešetřilo na zabezpečení. Měli bychom všichni stát za tím, aby naše osobní údaje nebyly zneužity. Protože ten, kdo doplatí nakonec na útoky nejsou jen cílené společnosti, či politické strany, ale my všichni.