CYBER SECURITY

Soukromí? Bezpečnost?

Současná společnost je doslova závislá na informačních a komunikačních technologiích. Představte si, že by z ničeho nic došlo ke kolapsu těchto technologií a služeb. Pro značnou část populace by to mělo katastrofální následky. O zranitelnosti a závislosti moderního světa na informačních technologiích se přesvědčujeme pokaždé, když dojde ke kybernetickému útoku. Nabízí se tedy otázka, jestli jsme skutečně moderní společností? Možná by dnes obstála lepší definice - online společnost. Jsme neustále připojeni, ať chceme nebo ne, před mobilem, počítačem, internetem atd, se neschováte, prostě jsme si zvykli. Technologie se neustále upravují, vylepšují, zkoumají z jedné, z druhé strany… Ale přiznejme si, v řadě případů zjišťujeme, že některé skutečně ani nepotřebujeme.

Informace a data představují značný potenciál, a svým způsobem dokáží rozhodovat o bytí či nebytí společnosti. Existuje vůbec nějaké soukromí? Je třeba si uvědomit, že čím více budeme horlivě hltat každou IT novinku, tím více dat o nás tyto technologie budou sbírat a sdílet. Možná odvážné tvrzení, ale soukromí je v tomto ohledu přežitek, máme sice všudypřítomnou svobodu, ale platíme za ni svými daty a stáváme se zranitelnějšími. Rozhodně to není pokyn k odpojení se ze všech “internetů” ani nemusíte propadat digitální hysterii, ale je třeba se nad tím aspoň trochu zamyslet. Do domu si zloděje také nepustíte, ale do svého počítače ano?

Kyberprostor nemá konec ani začátek, ovšem je závislý na reálném světě. Kybernetická bezpečnost je oblast, která je pro řadu organizací klíčová, a proto se k této oblasti musí přistupovat zodpovědně a především systematicky s dlouhodobým plánem. Obecná definice kybernetické bezpečnosti říká, že se jedná o ochranu počítačových systémů a sítí před krádeží anebo poškozením jejich HW, SW nebo elektronických údajů. Nutno dodat, že absolutní bezpečnost neexistuje, vždy tu bude existovat riziko či hrozba útoku. Primární cíl kybernetické bezpečnosti je, aby se možné riziko či hrozba snížilo na minimum. Existují tři prvky, které jsou schopny kybernetickou bezpečnost nastolit, tedy jejich vzájemná integrita to dokáže. Lidé - Technologie - Procesy. Lidé představují zásadní prvek v kybernetické bezpečnosti, protože sami sebe můžeme pasovat do role strůjce této bezpečnosti, příjemce (pravidla bezpečnosti), subjektu, který je třeba chránit anebo dokonce můžeme představovat ono riziko či hrozbu v rámci vytváření kybernetické bezpečnosti. Technologie samy o sobě nedokáží vyřešit všechny naše problémy, ale jsme za ně schopni vynaložit nemalé finanční prostředky. Aby bylo možné

zajistit kybernetickou bezpečnost je zcela nutné technologie aktualizovat, aby byly schopny reagovat na změny, které se s vývojem IT pojí. Můžeme si myslet, že technologie hrají v kybernetické bezpečnosti zásadní roli, ovšem zdání klame. Mnohem významnější je oblast dobře nastavených procesů a uživatelů, kteří umějí procesy aplikovat, popřípadě přizpůsobit situaci a hlavně (a to je velmi zásadní) předem nastavená pravidla dodržovat. Nastavení takových procesů a jejich následná údržba představuje tu nejnáročnější část při budování kybernetické bezpečnosti. Je zcela na místě, aby se prováděly simulace kybernetických útoků, a to právě z důvodů možných dopadů. Penetrační testování umožňuje nalézt chyby v nastavených procesech (např. odhalení slabých stránek infrastruktury) a předejít tak těmto nežádoucím dopadům. Mezi nesporné benefity penetračních testů se řadí především ochrana zákazníků, obchodních partnerů a třetích stran, ochrana reputace firmy, zmapování aktiv a samozřejmě soulad s různými standardy (OWASP, NIST, FIPS). Existují různé typy a strategie penetračních testů, například “Black Box” Test, jedná se o test, kdy útočník nemá žádnou informaci o systému, přičemž tento test nejlépe dokáže simulovat reálný útok. “Grey Box” Test, útočník má částečná práva a informace o systému anebo “White” Box” Test, kdy útočník má veškerá kompletní práva (admin práva).

V oblasti kybernetické bezpečnosti máme mnoho zkušeností, v tomto směru tedy držíme krok s dobou a sledujeme nejnovější trendy. Pomáháme velkým i malým společnostem, včetně prestižních bank, zvýšit jejich bezpečnost. Vždy jsme připraveni spolupracovat, vyhodnotit případná rizika a navrhnout adekvátní řešení.

Budování a udržování kybernetické bezpečnosti bychom mohli přirovnat k nikdy nekončícímu koloběhu rizik či hrozeb, které je potřeba rozšířit o podpůrné procesy, jako je například edukace lidí v této oblasti. Lidé by měli pochopit alespoň základní pravidla a principy, které se k tomuto tématu vztahují, měli by rozumět základním funkcím počítačových systémů, které denně používají, a také by měli rozumět aplikacím, které využívají.