MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

POLICEJNÍ AKADEMIE ČR

AFCEA

KYBERNETICKÉ ÚTOKY

Rok 2012 má být podle Mayského kalendáře koncem světa. Poslední datum v Mayském kalendáři je 21. prosince 2012. V souvislosti s Anonymus, kybernetickou válkou a současnou turbulencí okolo svobody na internetu si dovolím tvrdit, že staří Mayové možná předpověděli **konec světa, ale nikoliv hmotného, ale informačního.**

My jsme Anonymus. Jsme Legie. Neodpouštíme. Nezapomínáme. Můžete nás očekávat. Přidejte se k nám. Těmito slovy končí prakticky každá výzva hnutí Anonymus, jehož vznik se datuje někam k roku 2003. Anonymus je skupina hackerů, kteří zabraňují přístupu na vybrané weby, a podle svých vlastních slov z nich i kradou data. Nechme teď stranou, že by spíše sedělo označení cracker, médii zažitá terminologie pro takové chování je hacker.

Ve svých posledních spotech vyhlásili ANONYMUS **první oficiální kybernetickou válku**, vyzývají k účasti na svých protestech a dávají široké veřejnosti k dispozici postupy jak napadnout vybrané weby.

Je otázkou, zda Ratifikační proces Obchodní dohody proti padělatelství ACTA byl v České republice pozastaven nejen kvůli tomu, že dokument je třeba ještě důkladně analyzovat a to nejen proto, že smlouvu doprovází ve světě i v ČR vlnu útoků a i jiného odporu.

Zajištění kybernetické bezpečnosti státu je jednou z klíčových výzev současné doby. Lisabonský summit NATO uskutečněný v roce 2010 mimo jiné zdůraznil nutnost řešení této problematiky jak na mezinárodní úrovni, tak i na úrovni národní. Bezhraničnost a všudypřítomnost kybernetických hrozeb vyžaduje intenzivní mezinárodní spolupráci a také intenzivní úsilí při zajišťování kybernetické bezpečnosti jednotlivých států.

Chtěl bych podotknout, že v rámci právního pořádku České republiky není do současné doby právní úprava, která by uceleně upravovala problematiku kybernetické bezpečnosti.

Dne 19. října 2011 přijala vláda České republiky usnesení č. 781 o ustavení Národního bezpečnostního úřadu gestorem problematiky kybernetické bezpečnosti a zároveň národní autoritou pro tuto oblast. Na základě přijatého usnesení vzniklo Národní centrum kybernetické bezpečnosti, jako součást Národního bezpečnostního úřadu, se sídlem v Brně.

Národní bezpečnostní úřad v současné době předložil věcný záměr zákona o kybernetické bezpečnosti k připomínkám širší, i odborné veřejnosti.

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

CO JE KYBERNETICKÝ ÚTOK

Kybernetickým útok je činnost, při které je záměrem útočníka získat informace, negativně ovlivnit nebo i převzít kontrolu nad prvky infrastruktury systému kybernetického prostoru. Základem kybernetické obrany systémů je podle mého názoru dohled prvků infrastruktury systémů kybernetického prostoru, management bezpečnostních incidentů, pravidelné provádění auditů, hodnocení zranitelností systémů kybernetického prostoru nebo provádění penetračních testů.

Předmětem kybernetické bezpečnosti je nutnost zabezpečit bezpečí v kyberprostoru, dále ochrana dat před zničením, krádeží a zneužitím zločinnými hackery (státními, ale i soukromými) a prioritou je rovněž ochrana osob, jichž se data týkají.

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

PŘEDPOKLÁDANÉ CÍLE KYBERNETICKÝCH ÚTOKŮ

Kybernetičtí útočníci se v letošním roce zaměří hlavně na politicky motivované útoky, demonstrace kybernetické války a vysoce cílené útoky na firmy fungující v určitém oboru. Vyplývá to z nejnovější prognózy společnosti McAfee počítačových hrozeb v tomto roce (2012 Threat Predictions). Budou tak pokračovat trendy z loňského roku, typy útoků rostoucí v loňském roce se letos stanou dominantními.

Hlavním cílem kybernetických útočníků bude podle mého názoru testování možností těchto útoků. Až dosud vlády vyspělých zemí chránily především své vládní a vojenské sítě. V současné době by si měly uvědomit i míru škod, které mohou způsobit akce proti další kritické infrastruktuře, zejména rozvodným sítím a bankovnictví.

Jedná se o typy útoků, které způsobí problémy a škodu zejména v každodenním životě všech uživatelů, tedy státu, právnických osob, ale i jednotlivců

- Mezi hlavní rizika spojená s nečinností při zabezpečení kybernetické bezpečnosti se řadí nárůst kybernetických útoků, výrazné materiální škody, ohrožení kritické infrastruktury státu a v neposlední řadě i neplnění mezinárodních závazků České republiky včetně závazků plynoucích ze smluv o ochraně investic.
- Útoky na systémy rozvodných sítí. Jedná se o systémy, na nichž závisí velké množství lidí v každodenním životě, často jsou ale vzhledem ke svému významu zabezpečeny nedostatečně.
- Zatížení E-mailového provozu „legálními spamy". Množství spamu sice klesá, nicméně toto místo zaplní inzerenti, kteří budou houfně používat seznamy adres, jejichž uživatelé dali (vědomě či nevědomě) k zasílání souhlas, samozřejmě za vydatné spolupráce hackerů.

- Výrazně vzroste také množství útoků na mobilní bankovnictví. Útočníci se v těchto případech budou častěji zkoušet obejít samotné PC a cílit útoky přímo na bankovní aplikaci v mobilním zařízení, které není dostatečně (např. šifrování vzájemné komunikace apod.).
- Podvodníci s většími technickými dovednostmi se zaměří na vestavěné systémy (v automobilech, lékařských zařízeních, GPS, fotoaparátech či tiskárnách).
- Hackeři se více zaměří i na virtuální měny, tedy na on-line peněženky, kreditní karty a prováděné internetové obchody. Tyto transakce a přístup k příslušným účtům často nebývají rovněž chráněny šifrováním, proto pro útočníky může být výnosnější získat virtuální měnu a až tuto dále směnit za peníze či zboží.

- Kybernetické útoky velkého rozsahu mohou vypadat v místních podmínkách jako četné, opakující se bagatelní incidenty v sítích, ale až vyhodnocení informací z větší části informační nebo komunikační infrastruktury může v takových případech přinést adekvátní identifikaci kybernetického útoku, jeho rozsahu a nebezpečnosti.
- K dalším trendům tohoto roku bude patřit využívání podvržených digitálních certifikátů. Hacktivismus v on-line světě bude stále více propojen i s politickými aktivitami ve světě fyzickém. Více než dříve budou tyto akce mířit proti politikům, soudům, policejním složkám, ale i vrcholným manažerům. Předpokládám, že v roce 2012 také dojde k prvním, ukázkovým akcím v oblasti kybernetické války, které však budou maskovány kriminální činností.

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

SCÉNÁŘ KYBERNETICKÉHO ÚTOKU

Pokud se začne mluvit o cílech kyberútoku, většina lidí se domnívá, že se jejich osoby netýká, a že to je problém státu, respektivě činností, mající vztah k obraně či bezpečnosti státu. Takové přemýšlení je však v rámci kybernetických hrozeb vážným rizikem.

Kybernetický útok musí být zákonitě skrytý nebo alespoň do poslední chvíle skrývaný. Opravdový cíl nesmí být odhalen dříve, než se vytvoří dostatečné předpolí pro jeho efektivní zasažení. Zde je samozřejmě vidět paralela s běžnou válečnou taktikou a hacker, i když útočí jinými zbraněmi, je v tomto smyslu stejným bojovníkem jako voják v poli. Principy boje se tak podobají klasické konvenční válce. Proto se lze v budoucích konfliktech připravit na to, že vedle klasického válečného konfliktu bude docházet i k útokům na významné komunikační a informační body daného státu. Umím si představit, jak totálně paralyzovat vyspělý stát skrze kybernetickou válku. Ale jak praví klasik, štěstí přeje vyvoleným, a tak jsem si dal do souvislosti s předchozími skutečnostmi i informaci, kterou jsem nedávno zaslechl od odborníka na kybernetickou bezpečnost a to, že jeden nejmenovaný stát pořídil pro svoje potřeby poštovní holuby v řádu za desítky milionů korun.

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

V rámci kybernetického boje dochází ke směřování útoků do oblasti e-govermentu, tj. na aplikace propojující ministerstva státu s občany. Útoky jsou maskované a přicházejí přes běžných, domácích uživatelů v napadeném země. Napadeny a vyřazeny jsou veškeré aplikace ministerstev, dochází k průnikům do jednotlivých řídících informačních systémů ministerstev. Další skupina profesionálních hackerů útočí taktikou souběžného útoku na všechny banky státu, včetně banky národní. Tím dochází k úplnému zastavení obchodů a zablokování bankovních služeb státu, v rámci dalších aktivit pokračuje rozsáhlý kybernetický útok na silová ministerstva a zdravotnictví se snahou vyřadit kompletně jejich informační systémy (policejní registry, taktické a informační systémy, zdravotnické zabezpečení apod.). Dochází k částečnému narušení informační role v kyberprostoru státu, k odstavení zdrojů elektrické energie, (např. imitací havárie na jaderném bloku, vzdáleným přebráním správy zařízení, apod.). Narušení sítě integrovaného záchranného systému vyvolává všeobecnou paniku souběžně s narušením hromadných sdělovacích prostředků.

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Dalším úkolem kyberválečníků je zasadit poslední drtivý úder komunikační soustavě státu (mobilní operátoři, zprostředkovatelé internetových služeb, apod.) a uzlovým bodům jednotlivých existujících sítí. Tím jsou narušeny komunikační, bezpečnostní a podpůrné role v kyberprostoru státu. Možnou variantou kybernetického útoku je pouhé narušení měnového a finančního systému státu spojeného s dezinformační kampaní (např. připravované měnová reforma, devalvace apod.) a s vyvolaným, následným runem na banky.

K zajištění kybernetické bezpečnosti a odpovídajícímu zajištění práva na informační sebeurčení prostřednictvím přístupu k fungujícím službám informační společnosti je nutno zpracovávat informace o výskytu kybernetických bezpečnostních událostí z co největšího množství zdrojů. Ze stejného důvodu je třeba koordinovat ochranná opatření. Služby informační společnosti se totiž vyznačují svým síťovým charakterem, přičemž i rozsahem nepatrný prvek sítě může závažným způsobem ovlivňovat její ostatní části, to dokonce často i bez ohledu na geografickou blízkost.

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

ÚKOLY PŘI OCHRANĚ KYBERNETICKÉHO PROSTORU

- Koordinace protiopatření pro případ IT bezpečnostních incidentů v kritické infrastruktuře.
- Sběr informací o závažných bezpečnostních incidentech.
- Koordinace vyplňování bezpečnostních děr v kritických počítačových systémech.
- Řešení informačně-bezpečnostním incidentů ve spolupráci s vlastníky a provozovateli postižených částí, telekomunikačními operátory, poskytovateli internetových služeb a se státními orgány.
- Budování a rozšiřování znalostí veřejnosti ve vybraných oblastech informační a kybernetické bezpečnosti.
- Kooperace se zahraničními organizacemi a prezentace České republiky v oblasti informační bezpečnosti na mezinárodní úrovni.

- Vybudování schopnosti bránit se kybernetickým útokům.
- Dosažení mezinárodního konsensu o normách chování v kyberprostoru.
- Omezení zranitelnosti vládních systémů a kritické infrastruktury.
- Podpora výuky profesionálů v oblasti kybernetické bezpečnosti.
- Posilování vymahatelnosti práva v oblasti kybernetické bezpečnosti.
- Zlepšení prevence a vybudování obecného povědomí.
- Zvýšení povědomí v privátním sektoru.
- Vytváření personálu odborné správy v oblasti bezpečnostních systémů informačních a komunikačních technologií.
- Porozumět taktikám útočníků, jejich technikám a procedurám, které umožní přetvořit obranná opatření do vhodných podob.

- Být připraven zabránit útoku či odpovědět tak rychle, jak je možné – v případě kompromitace.
- Preferována by měla být prevence, ale nutností je také detekce a vhodná odpověď na útok.
- Mít k dispozici nouzový plán k tomu, co dělat v případě, když se stanete obětí kybernetického útoku.
- Přesvědčit se, že dodavatelé v rámci kritických infrastruktur nejsou kompromitováni a mějte k dispozici vhodná opatření v případě, že jejich systémy budou narušeny.
- Národní kritická infrastruktura nesmí být plně závislá na internetu, ale musí být operabilní i v případech, kdy přijde krize kybernetické bezpečnosti.

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Dotazy, otázky ?

Děkuji za pozornost