ZAJIŠŤOVÁNÍ KYBERNETICKÉ BEZPEČNOSTI VOLEB A VOLEBNÍHO PROCESU

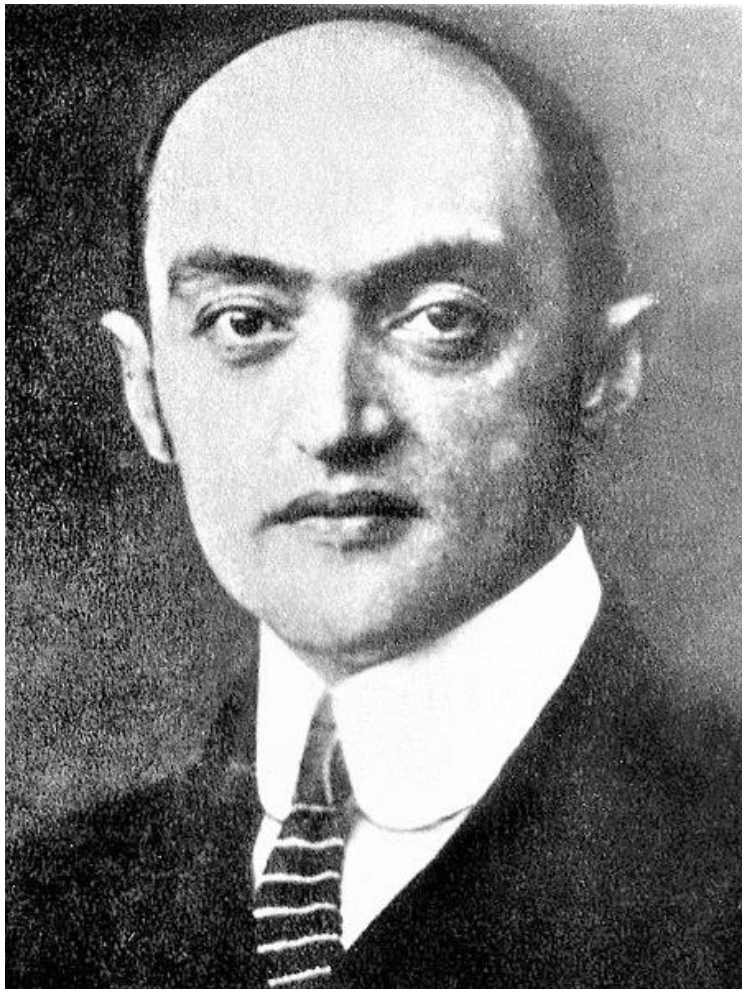
Petr Novotný

Národní úřad
pro kybernetickou
a informační bezpečnost

OBSAH PŘEDNÁŠKY

1) Role voleb v demokratickém státě
2) Role kybernetického elementu ve volbách a volebním procesu
3) Cíle, aktéři, motivy
4) Přehled incidentů
5) Jižní Korea – doplňovací volby v Soulu 2011
6) Ukrajina – prezidentské volby 2014
7) USA – prezidentské volby 2016
8) Francie – prezidentské volby 2017
9) Vytvrzování volebního procesu v ČR

VOLBY V DEMOKRATICKÉM STÁTĚ



Josef Alois Schumpeter

Democracy is just a system in which rulers are selected by competitive elections.

ROLE KYBERNETICKÉHO ELEMENTU VE VOLBÁCH A VOLEBNÍM PROCESU

- Trend přesouvání prvků volebního procesu do kyberprostoru.
- Estonsko jako „extrémní“ příklad.
- Využití volebních automatů (USA, Brazílie).
- Přenos a prezentace volebních výsledků prostřednictvím kyberprostoru.

MOTIVY A AKTÉŘI

Motivy

1) Pozměnění samotných výsledků
2) Ovlivnění volebních výsledků
3) Narušení důvěry ve volební systém

Aktéři

1) Politické strany
2) Státy
3) Skupiny a jednotlivci jednající v zájmu státu
4) Hacktivistické skupiny
5) Kriminální skupiny

CÍLE

1) Politické strany
2) Politici
3) Média
4) Veřejné instituce
5) Volební proces

Country	Year	Method used	Target	Attacker
Bulgaria	2015	DDoS	Central election commission, ministries	unknown
Montenegro	2016	DDoS	media, political parties, mobile network operator	unknown
Philippines	2016	defacement, data theft	election commission websites, voters database	Anonymous Phillippines, LulzSec Phillippines
France	2017	not published	Socialist party	origin abroad
		??? (supposedly social engineering)	En Marche! Party	supposedly Russians (APT 28)
Ghana	2016	defacement	National election commission	unknown
South Korea	2011	DDoS	National election commission, opposition candidates	probably members of government party
Malaysia	2013	DDoS	media and opposition candidates	unknown, government among suspects
Nigeria	2015	defacement	Nigerian election commission	Nigerian Cyber Army
Russian Federation	2011	DDoS	independent media	unknown
	2012	DDoS	web cameras in polling station	unknown
Taipei	2015	spear phishing, backdoor	media and DPP members	China, group APT16
Slovakia	2014	defacement	web presentation of candidate	unknown
	2014, 2016	DDoS	web presentation	unknown
Tunisia	2014	not published	voters registration system	unknown
Ukraine	2014	DDoS	Ukraine election commission	Kyberberkut group, traces show Russian support/influence
US	2015-2016	spear phishing, malware	Democratic party	supposedly Russian Federation, APT 28 and APT 29
	2016	spear phishing, malware	suppliers, clerk	supposedly Russian Federation, APT 28
	2016	unknown	database of election commission	supposedly Russians
Cambodia	2018	spear phishing	Government entities overseeing election	TEMP.periscope, probably China

JIŽNÍ KOREA

- Útoky se odehrály v roce 2011 v rámci **doplňovacích voleb na post starosty Soulu.**
- Proběhly útoky na dva cíle:
  1) Webové stránky Národní volební komise
  2) Webové stránky kandidáta Demokratické strany

- Oba útoky měly **formu DDoS útoku** a vyřadily napadené stránky, nebo alespoň výrazně omezily jejich dostupnost.

JIŽNÍ KOREA

- Útok na Volební komisi ráno v den voleb – **znepřístupnění informací o volebních místech.**
- Z útoku **obviněn 27 letý asistent** jednoho z poslanců vládní strany.
- Měl být údajným organizátorem útoku, ale vzhledem k potřebným zdrojům se to **nezdá jako pravděpodobné**.
- Reálná možnost, že vystupoval jako prostředník, aby kryl výše postavené členy strany.
- Poslanec, kterému Gong asistoval, odstoupil z funkce a opustil stranu.

UKRAJINA – situace v zemi

- Předčasné prezidentské volby se konaly **25. května 2014.**
- Od února je **Krym okupován Ruskou federací**, od začátku dubna probíhá konflikt na východě země.
- Hlasování bylo v některých oblastech obtížné či nemožné.
- Průzkumy předpovídaly jasné **vítězství Petra Porošenka.**

UKRAJINA – útok na infrastrukturu

- Čtyři dny před volbami proběhl úspěšný útok skupiny **Kyberberkut**.
- Její členové **pronikli do systému sloužícího k elektronickému sčítání hlasů** a poškodili ho.
- Útok spojen s údajným **defacementem** webu ministerstva vnitra.
- Systém se podařilo obnovit ze zálohy.

UKRAJINA – POKUS O MANIPULACI VÝSLEDKŮ

- Těsně před ukončením hlasování došlo k **odhalení malware v síti centrální volební komise**.
- Malware byl **včas odstraněn**, ale jeho přesný účel není znám.
- Paralelně proběhl krátký defacement stránek komise. **Vítězem v něm byl označen Dmytro Jaroš**.
- Pozměněné výsledky stihla odvysílat ruská televize Russian Channel One.
- Jako pachatel označena skupina **Kyberberkut.**

UKRAJINA – útok na infrastrukturu 2.0

- Po ukončení voleb došlo 26. května ráno k **DDoS útoku na infrastrukturu přenášející výsledky do centrály**.
- Útok trval asi dvě hodiny.
- Obešel se bez vážnějších následků.
- Společnost Arbor Networks přisoudila útok skupině **Kyberberkut**.

UKRAJINA - útočníci

- Pro-rusky orientovaná hackerská skupina.
- Nešlo o ojedinělou akci.

UKRAJINA - útočníci

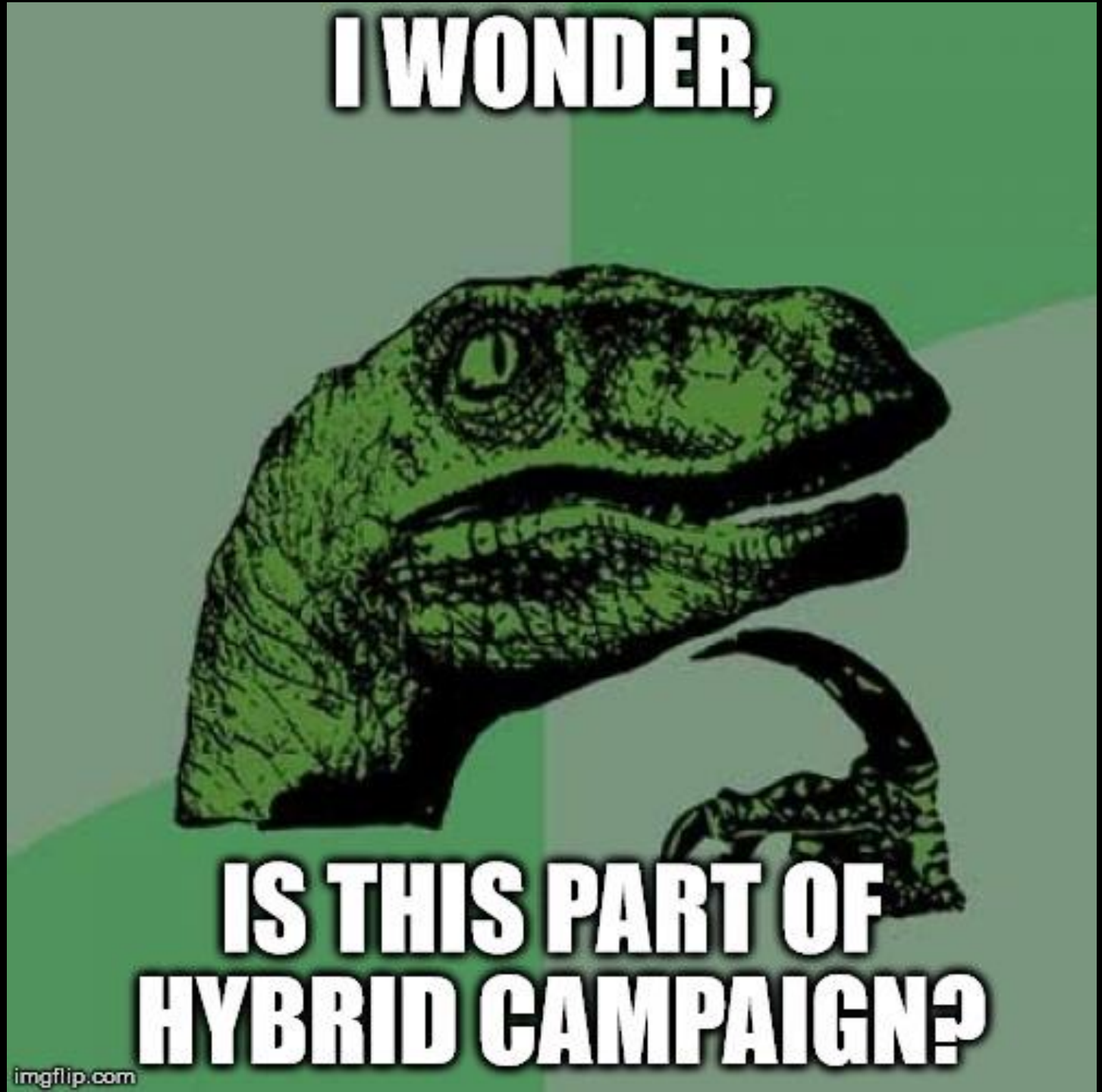
- Při útoku proti systémům volební komise měla skupina využít **zranitelnost nultého dne**.
- Jde o velmi sofistikovaný útok, kterého dle vyjádření expertů není hacktivistická skupina **bez podpory státní entity schopna.**
- Podezřelá je i rychlost zveřejnění defacementu stránek komise.
- Některé zdroje mluví o **pravděpodobném zapojení APT 28** do útoků.

UKRAJINA - útočníci

- Pro DDoS útoky **využívají sympatizanty**, kteří si stáhnou nástroj, s pomocí nějž se mohou útoků jednoduše účastnit.
- V lednu 2015 odhalil údajnou identitu některých členů ukrajinský Pravý sektor. Není však jasné, zda jde skutečně o čelní představitele.
- Defense Intelligence Agency uvádí, že jde o **hacktivisticou skupinu sponzorovanou Ruskem**.

UKRAJINA

- **Rozličné vektory** útoků i jejich terče.
- Můžeme mluvit o **rozsáhlejší kampani**.
- Nutné **vnímat (nejen) v kontextu** konfliktu na Ukrajině a období, kdy útoky proběhly.
- Cíleno na specifické publikum – **podpoření ruského narativu o rozmachu krajní pravice**.
- Znedůvěryhodnění institucí a volebního procesu.


I WONDER,
IS THIS PART OF HYBRID CAMPAIGN?
imgflip.com

SPOJENÉ STÁTY

- Pravděpodobně snaha ovlivnit výsledek voleb a narušit důvěru v tento demokratický prvek.
- Tři dimenze:
  A. Útok na Demokratickou stranu
  B. Útok na volební infrastrukturu
  C. Informační operace

SPOJENÉ STÁTY AMERICKÉ

A. Útok na Demokratickou stranu

- Dle některých zdrojů se do systémů demokratické strany nabourali postupně dva útočníci:
  a) **APT 29** (Cozy Bear, The Dukes)
     - Proniknutí do systému v červnu 2015
  b) **APT 28** (Fancy Bear, Pawn Storm, STRONTIUM)
     - Proniknutí do systému v dubnu 2016
- Prvotním motivem pravděpodobně špionáž, APT 28 už ale vedla útok v souvislosti s nadcházejícími volbami.

SPOJENÉ STÁTY AMERICKÉ

- Vektorem útoku zejména **spearphishing**.
- Cílem infiltrace do rozličných systémů Demokratické strany zejména **zisk dokumentů**, které by mohly být zveřejněny.
- Cílili zejména na vysoce postavené představitele.
- Po úspěšné infiltraci byly útočníci schopni registrovat **veškeré údery na klávesnici a pořizovat prinscreen obrazovky.**

SPOJENÉ STÁTY AMERICKÉ

- Využití vlastního malware (X-agent, X-tunnel)

  ⟹ znak sofistikované skupiny.
- Udržela si přístup do některých systémů i po opatřeních přijatých bezpečnostní společností.
- Pro zveřejnění ukradených dat **založena stránka DCLeaks**.
- Další materiály zveřejněny skrze fiktivní entitu Gucifer 2.0 poté, co DNC oznámila hackerský útok.

SPOJENÉ STÁTY AMERICKÉ

Search Term(s)
“some hundred sheets”
“some hundreds of sheets”
dcleaks
illuminati
широко известный перевод [widely known translation]
“worldwide known”
“think twice about”
“company’s competence”

Worldwide known cyber security company [Company 1] announced that the Democratic National Committee (DNC) servers had been hacked by “sophisticated” hacker groups.

I’m very pleased the company appreciated my skills so highly))) [. . .]

Here are just a few docs from many thousands I extracted when hacking into DNC’s network. [. . .]

Some hundred sheets! This’s a serious case, isn’t it? [. . .]

I guess [Company 1] customers should **think twice about company’s competence**.

F[***] the **Illuminati** and their conspiracies!!!!!!!!! F[***] [Company 1]!!!!!!!!!

SPOJENÉ STÁTY AMERICKÉ

B. Útok na volební infrastrukturu

- Vektorem útoku především spearphishingové útoky.
- Veden jak na úředníky jednotlivých států, kteří se podíleli na zajištění volebního procesu, tak také na soukromé společnosti.
- V případě soukromých společností útočníci aktivně hledali zejména informace a používaném software a hardware.
- Dle samotných USA se GRU podařilo získat statisíce osobních údajů z databáze voličů.

SPOJENÉ STÁTY AMERICKÉ

C. Informační operace

- Rozsáhlé operace vedeny společností **Internet Research Agency**.
- Sídlo v Petrohradě, vedena oligarchou blízkým vládě.
- Struktura „standardní“ společnosti:
  a) Oddělení grafiky
  b) Oddělení datové analýzy
  c) Search-engine optimalization
  d) IT oddělení
  e) Ekonomické oddělení
- Sama společnost svoji činnost definovala jako „**informační válku pro USA.**“

SPOJENÉ STÁTY AMERICKÉ

- **Cílem činnosti šířit nedůvěru vůči kandidátům stejně jako obecně v politický systém**.
- Při své činnosti se řídili strategií. Podpora některých kandidátů (Trump, Saunders), negativní kampaň proti dalším.
- Zaměření na tzv. „**purple states**“.
- Cíleno na menšiny, radikální skupiny.
- V rámci své činnosti do USA i vycestovali.
- Na sociálních sítích **vystupovali zejména jako americké organizace.**

SPOJENÉ STÁTY AMERICKÉ

- United Muslims of America
- Blacktivist
- Tennessee GOP

- Secured Borders
- Army of Jesus
- Hearth of Texas
- South United

SPOJENÉ STÁTY AMERICKÉ

- Svoji aktivitu na sociálních sítích dále **propagovali s pomocí** zakoupené **reklamy.**
- Útrata v řádech tisící dolarů měsíčně s pomocí účtů na PayPalu.
- Svůj vliv využili ke **svolávání demonstrací**.
- Pečlivé sledování metrik (followers, clics, visits, etc.)
- Účty, které obsah **zveřejňovaly**

- Účty, které obsah dále **propagovaly**
- Po volbách využili svých účtů ke svolání demonstrací jak na podporu Donnalda Trumpa, tak také proti němu.

FRANCIE

- Historicky doložený **případ vměšování** již z roku **1974**
- Dle NSA a US Cyber Command se v roce 2017 skupina ruských hackerů pokusila proniknout do volební infrastruktury.
- **Informační moratorium** začíná 44 hodin před otevřením volebních místností.
- Nevztahuje se na sociální sítě.
- Dva dny před začátkem voleb se 9GB dat objevilo na Pastebin.
- Na první pohled bezproblémové dokumenty.
- Macronův tým stihl vydat prohlášení, že mezi uniklými e-maily je množství podvržených.

FRANCIE

- **#MacronLeaks** se objevil v USA, následně ho amplifikovaly automatické účty, které pomohly jeho rozšíření.

FRANCIE

- Macronův tým zvolil **unikátní obranu**:
  1) Zahltil útočníky množstvím přístupových údajů
  2) Některé falešné dokumenty byly útočníkům podstrčeny cíleně
  3) Novinářům byla předána data pro ověření obsahu e-mailů
  4) Objevena azbuka v metadatech dokumentů
- Cílem útočníků poškození E. Macrona a jeho strany v očích voličů.

VYTVRZOVÁNÍ VOLEBNÍHO PROCESU V ČR

- Volby organizovány **Českým statistickým úřadem.**
- Roli v procesu voleb dále má:
  - ✓Ministerstvo vnitra
  - ✓Samospráva
  - ✓Ministerstvo zahraničních věcí
  - ✓Soukromé subjekty
- NÚKIB nemá zákonem zakotvenou roli ve volebním procesu.

VYTVRZOVÁNÍ VOLEBNÍHO PROCESU V ČR

Pracovní skupina pro ochranu voleb

- Ustanovena v roce 2017 jako reakce na incidenty v zahraničí.
- Vedena Ministerstvem vnitra.
- Mezi další členy patřili například zpravodajské služby či ČSÚ.
- Cílem zaměřit se na bezpečnost volebního procesu ve světle nadcházejících parlamentních a prezidentských voleb.

VYTVRZOVÁNÍ VOLEBNÍHO PROCESU V ČR

- Vzájemná spolupráce mezi ČSÚ a NÚKIB vzešla právě na základě Skupiny.
- Časová osa spolupráce:

1) seznámení se s ICT komponentem voleb a jejich procesem ze strany NÚKIB
2) Identifikace slabých míst, možných vektorů útoku a míst k vytvrzení
3) Sdílení poznatků s ČSÚ, spolu s doporučeními
4) Penetrační testování vybraných ICT komponent
5) Školení zaměstnanců ČSÚ v oblasti kybernetické bezpečnosti
6) Diskuze nad možnými scénáři útoků
7) Spolupráce během incidentu v říjnu 2016
8) Zpětná vazba a dlouhodobá spolupráce

VYTVRZOVÁNÍ VOLEBNÍHO PROCESU V ČR

1) **seznámení se s ICT komponentem voleb a jejich procesem ze strany NÚKIB**
   - Klíčová vůle k vzájemné spolupráci
   - Nutnost porozumět volebnímu procesu jako celku, tedy všem dimenzím:
     a) Technické (Jaké technologie jsou využívány?)
     b) Procesní (Kdo je do procesu zapojen?)
     c) Organizační (Jak jsou volební výsledky předávány do centrály ČSÚ?)
   - **Nestačí porozumět pouze technickému aspektu!!!**

VYTVRZOVÁNÍ VOLEBNÍHO PROCESU V ČR

2) Identifikace slabých míst, možných vektorů útoku a míst k vytvrzení

- Sběr informací o incidentech, které se odehráli v zahraničí:
  - ✓otevřené zdroje
  - ✓spojenci a partneři
  - ✓konzultace expertů
- Soustředění se na:
  - ✓motivace, cíle a terče útočníků
  - ✓modus operandi útočníků
  - ✓vektory útoku
  - ✓zvolená obrana včetně silných a slabých míst
- To vše vedlo k identifikaci slabých míst ve volebním procesu ČR.
- Důležitá je schopnost myslet jako útočník.

VYTVRZOVÁNÍ VOLEBNÍHO PROCESU V ČR

3) Sdílení poznatků s ČSÚ, spolu s doporučeními

- Nestačí slabá místa jen sdílet, byla rovněž dána doporučení k jejich odstranění.
- Dlouhodobá doporučení

  (smlouvy s dodavateli)

  vs.
- Okamžitě aplikovatelná opatření

  (nastavení jednotlivých počítačů)

VYTVRZOVÁNÍ VOLEBNÍHO PROCESU V ČR

4) Penetrační testování vybraných ICT komponent

- Opět včetně zpětné vazby a doporučení.

5) Školení zaměstnanců ČSÚ v oblasti kybernetické bezpečnosti

- Součástí digitální hygiena ⟶ maximálně užitečná a aplikovatelná doporučení včetně živých ukázek.
- Další součástí případové studie kybernetických útoků na volební proces v zahraničí.

VYTVRZOVÁNÍ VOLEBNÍHO PROCESU V ČR

6) Diskuze nad možnými scénáři útoků

- Připraveno zaměstnanci NÚKIB.
- K přípravě scénářů byly nutné předcházející kroky – získání rozsáhlého povědomí.
- Diskuze měla komplexní charakter a pokrývala mimo jiné následující oblasti:
  - ✓ technickou
  - ✓ procedurální
  - ✓ organizační
  - ✓ mediální ad.

VYTVRZOVÁNÍ VOLEBNÍHO PROCESU V ČR

7) Spolupráce během incidentu v říjnu 2016

- Během voleb do PSP ČR v říjnu 2017 došlo k DDoS útoku na webovou prezentaci výsledků.
- I přes protiopatření byla nedostupná několik desítek minut.

8) Zpětná vazba a dlouhodobá spolupráce

- Kybernetické útoky na volební proces jsou realitou, kterou je nutné akceptovat a připravit se na ni.
- Nutná dlouhodobá spolupráce NÚKIB a ČSÚ.
- Každý ICT komponent, který bude hrát roli ve volebním procesu by měl být vybírat s přihlédnutím k bezpečnosti.

VYTVRZOVÁNÍ VOLEBNÍHO PROCESU V ČR

- NÚKIB se rovněž podílel na edukaci zástupců politických stran i zástupců prezidentských kandidátů.
- Důraz kladen na digitální hygienu a okamžitě aplikovatelné postupy.
- Politické strany nejsou běžným „klientem“ Úřadu, ale při zabezpečení volebního procesu byl zvolen komplexní přístup.
- Strany jako slabým místem:
  - ✓nízké povědomí o kybernetické bezpečnosti obecně
  - ✓strany jsou menší subjekty, musí prioritizovat zdroje
  - ✓jsou zranitelné již díky své povaze

LESSONS LEARNED

- Začněte včas
- Whole-of-government přístup
- Zahrňte také politické strany
- Nezapomeňte na soukromé subjekty, pokud hrají důležitou roli
- Využijte scénáře a cvičení jako vhodné nástroje k přípravě na krizi.
- Budujte dlouhotrvající partnerství


IVANKA TRUMP
CYBERSECURITY
FREEMAIL
imgflip.com