Realita Slovenskej republiky z pohľadu NCKB SK-CERT

SECURITY DAYS 2021

Rastislav Janota

Director

National CERT of the Slovak Republic

National Security Authority

SK NBÚ CERT

O ČOM SA ROZPRÁVAME

	Social Engineering	Phishingy	Ransomware	APT
	Typický otvárací kanál väčšiny útokov	Typický cieľ veľkej časti útokov je zber rôznych údajov priamo alebo nepriamo užitočných	Neustále rastúca forma útoku s cieľom finančnéhl zisku (kyber kriminalita)	Typicky používané techniky štátnych aktérov s iným cieľom ako priamy finančný zisk
Občania	X	X	X	
Firmy	X	X	X	
Kritické firmy / verejná správa	X	X	X	X

- Samozrejme pre útoky sú kde je to možné a vhodné používané neošetrené (otvorené) zraniteľnosti v infraštruktúre obeti útoku, najčastejšie v kombinácii s údajmi získanými cestou sociálneho inžinierstva a/alebo phishingu
- Rôzne formy útokov vyžadujú rôznu úroveň schopností na strane útočníka
- Samostatnou kategóriou sú tzv. Supply Chain útoky

- Viditeľný nárast škodlivých aktivít v kybernetickom priestore (na internete)
  - Nárast vo všetkých sledovaných oblastiach
  - Najmä phishing a ransomware
  - Viacero úspešných odhalených Supply chain útokov
  - (Obsahovo) nová oblasť zneužívajúca pandémiu COVID-19
  - Nárast má dva základné dôvody
    - Mierne sa zlepšujúca detekčná schopnosť organizácii – proste vidia viacej
    - Objektívny nárast

- Z hľadiska aktérov
  - Zvýšenie aktivity najmä kriminálnych aktérov a politických (štátnych aktérov)
  - Vývoj odzrkadľuje trendy vo svete (kriminálny aktéri)
  - Meniaca sa politická situácia, ktorá vedie k zvyšovaniu najmä aktivít Ruska, Číny a Turecka v rámci Európy

POZOROVANIA 1

- Kľúčové pozorovania – závery zo sledovania situácie na Slovensku v roku 2020
  - Mierne sa zvyšujúci záujem firiem o riešenie problematiky vlastnej bezpečnosti – ale stále to je masívne pod aspoň trosku použiteľnou úrovňou
  - U časti firiem je viditeľný priam VÝRAZNÝ ODPOR k téme alebo k regulácii (a teda ku kontrole, ako dobre to robia) -> od niektorých firiem a problematických výrobcov silný politický lobbing
  - V komerčnom SK svete medzi PZS je zhruba 50-60% firiem, ktoré hovoria, že sa téme venujú už nejaký čas a teda by nemali mať problém. Ale potom príde audit a zistenia často ukazujú ako veľmi sa mýlili
    - Niekde je to pre nich reálne prekvapenie, berú audit ako dobrý návod na ďalšie zlepšovanie
    - Ale sú aj iné reakcie...
  - V drvivej väčšine organizácii neexistujú reálne ani základne procesy napr. Na včasné aktualizácie prevádzkovaných technológii prinajmenšom – ako výsledok máme dnes aj závažné incidenty s vektorom útoku cez neopatchované zariadenia s opravou dostupnou už od jari 2019 a pod...
  - Staré/zlé architektúry firemnej infraštruktúry, neexistujúca alebo neefektívna segmentácia a pod.
  - Masívne podcenenie (až ignorácia) zálohovacích postupov aj technickej infraštruktúry pre zálohovanie
  - Neexistujúce procesy, a aj kde sú implementované tak je existencia veľkého množstva výnimiek

POZOROVANIA 2

- Kľúčové pozorovania – závery zo sledovania situácie na Slovensku v roku 2020
  - Absolútna neochota verejne komunikovať incidenty zo strany obetí a takto prispieť k celkovému povedomiu
  - Cielené porušovanie zákonných povinností
    - Najmä povinnosti hlásiť incidenty
    - Ale tiež povinnosti riešiť incidenty
  - Celkové povedomie dokonca aj v sektore dodávateľov IT technológii a služieb je slabé

  - Chýbajú odborníci na problematiku bezpečnosti
  - Vidíme absolútny nezáujem (až odpor) zo strany kompetentných orgánov riešiť oblasť vzdelávania
  - Celá problematika vzdelávania KB (povedomie až po expertnú úroveň) je zo strany ministerstva školstva kompletne ignorovaná

  - Viac detailov je v Správe o kybernetickej bezpečnosti SR za rok 2020

KONKRÉTNE PRÍKLADY

- Za udalosť roka 2020 považujeme na svetovej úrovni prípad SOLAR WINDS
  - Je to druhý VEĽKÝ odhalený prípad Supply Chain Attack formy (po prípode NotPetya)
  - Obidva prípady mali fakt obrovský dopad, stopy vedú k tomu istému štátnemu aktérovi
- Na slovenskej úrovni
  - Viacero príkladov spomíname v zverejnenej správe o kybernetickej bezpečnosti SR za rok 2020
  - Závažné incidenty boli hlásené v rámci len časti sektorov
    - -> incidenty boli všade ale subjekty porušujú povinnosť hlásiť
    - -> rôzne vyspelé celé sektory
    - Najvyspelejšie sektory sú Bankovníctvo a Energetika
    - Najmenej vyspelé sektory sú Verejná správa a Elektronická komunikácia
    - Spiace sektory sú napr. Voda a atmosféra, Doprava a Priemysel
    - Hlásené incidenty boli aj v kategórii III – najvyššia kategória incidentu
  - Okrem Phishingu je v rámci SK nástup Vishingu (telefonické hovory ako začiatok incidentu)

AKO ĎALEJ?

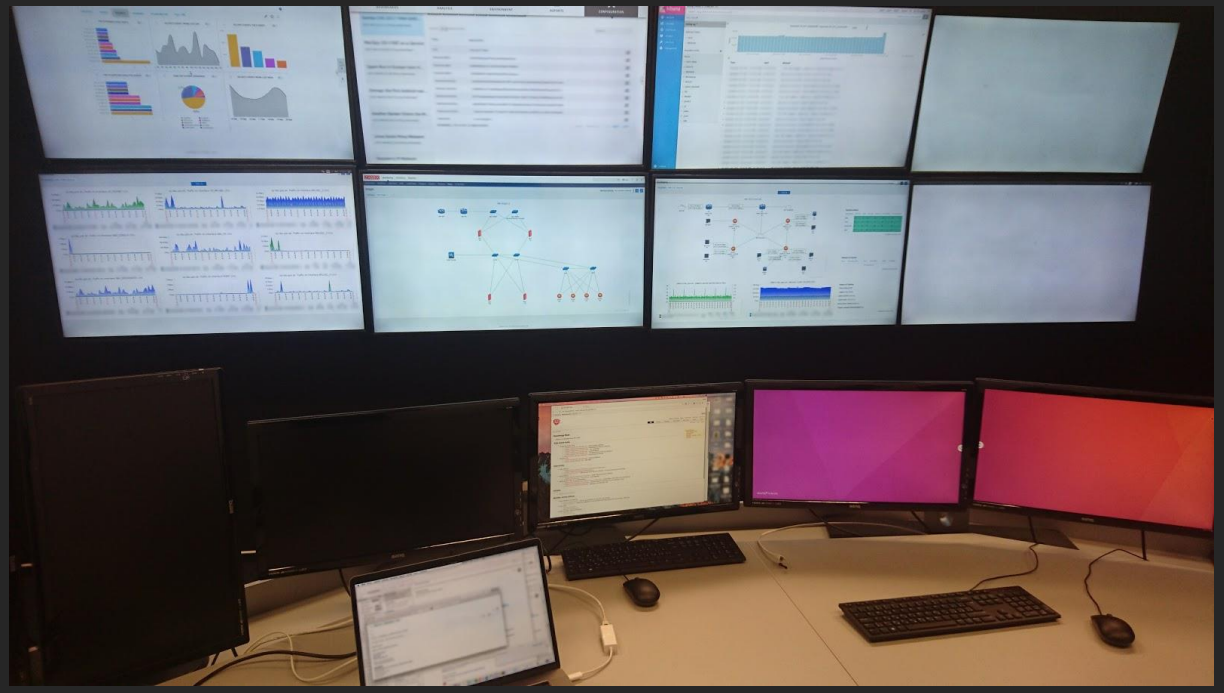
- Nedá sa predpokladať vylepšenie situácie – naopak
- Vývoj v roku 2021 (za prvých skoro 5 mesiacov) potvrdzuje zhoršujúcu sa situáciu
  - Ransomware na prvky KI, priemysel, verejnú správu a pod.
  - Výrazný rozvoj vishingu, pokračovanie phishingu
  - Zvyšujúca sa potreba na odborníkov tak, ako sa (dúfajme) bude zvyšovať povedomie o téme
  - Reálna ponuka odborníkov sa ešte dlho zvyšovať nebude, čiže nožnice sa viacej otvárajú k zlému
  - Bezpečnostná situácia vo svete a eu sa zhoršuje, kyber nástroje samostatne a ako súčasť hybridných aktivít
    - Rusko (Krym, Ukraina, Sputnik)
    - Čína (5G toolbox, Certifikácia kyber produktov a služieb)

Takže poznámka na záver:

Kybernetická bezpečnosť je téma NÁS všetkých, ak máme byť úspešní tak musíme každý priložiť ruku k dielu. A preto ďakujem aj ESETu za všetko čo v tejto téme robí (nehovorím teraz o produktoch ale o vzdelávaní, awarenesse, rozpoznávaní témy a pod.)

NATIONAL SECURITY AUTHORITY

ESET SECURITY DAYS



ĎAKUJEM

rastislav.janota@nbu.gov.sk

SK NBÚ CERT