AKO SA ZMENIL SVET ZA POSLEDNÉ MESIACE/ROKY?

Aká je úloha štátu v dnešnej kybernetickej bezpečnosti?
Nové vnímanie bezpečnosti – sme na neho vôbec pripravení?

Rastislav Janota

Riaditeľ

Národné centrum kybernetickej bezpečnosti SK-CERT

AKO TO BOLO PREDTÝM?

Vnímanie (kybernetickej) bezpečnosti štátom:

- Zákon o Kritickej infraštruktúre (tzv. prvky KI)
  - Prednostne fyzická ochrana vybraných prvkov v pár sektoroch
  - Najmä
    - Energetika
    - Doprava
    - Trochu telekomunikácii – ale len pri klasickej telefónnej službe
    - Časť priemyslu (farmácia, hutníctvo, chémia)
    - Časť zdravotníctva – pár nemocníc
    - Trošku bankovníctva
  - Celkovo veľmi formálny prístup bez **reálne zvýšenej ochrany**, a bez zmyslu

- Centrálne riadená bezpečnosť štátom (polícia, hasiči, armáda...)

AKO TO BOLO PREDTÝM?

Vnímanie kybernetickej bezpečnosti verejnosťou:

- Informačná bezpečnosť (termín kybernetická bezpečnosť sa skoro nepoužíval)
  - Vnímanie väčšinou ako zábava pre geekov (IT kockáčov),
  - alebo tiež ako čistý náklad pre firmy
  - => organizácie (manažment, majitelia) nevedeli uchopiť dôležitosť témy pre nich samotných

- Slovo bezpečnosť je vnímané hlavne na úrovni fyzickej bezpečnosti

- Koncept vnímania bezpečnosti verejnosťou:

Úloha vlády/štátu je chrániť občanov/služby

AKO JE TO (BY MALO RAZ BYŤ) TERAZ?

Postupná zmena rozmýšľania

- Zmena ešte nie ukončená, ale pracujeme na tom denne

Nové premisy

- Bezpečnosť nie je len fyzická ochrana
- Digitalizácia celého nášho života je na postupe
- Bez riešenej/vyriešenej bezpečnosti je digitalizácia veľkým rizikom

Čo sa mení?

- Pôvodný koncept DDI (Dostupnosť, Dôvernosť, Integrita) už nestačí
  - Treba pridať napr. Dôveryhodnosť
- Naozaj je vláda univerzálne zodpovedná za všetku ochranu?

- **Bezpečnosť začína byť vnímaná v širších súvislostiach**

AKO JE TO TERAZ?

Reálne je bezpečnosť (okrem fyzickej) ovplyvňovaná

- Zraniteľnosťami (konštrukčnými, chybami v programe a pod) v IT produktoch
  - Novými (neznámymi) ale aj známymi
  - Nechcenými aj (niekedy) chcenými
  - Neochotou/neznalosťouj majiteľa/prevádzkovateľa infraštruktúry riešiť tieto zraniteľnosti
    - Aktualizáciou produktov (ak existuje a funguje správne)
    - Inými opatreniami (ak aktualizácie nie sú možné z rôznych príčin – neexitujú alebo nefungujú dobre a pod.)

- Zabudovanými chybami –napr. prostredníctvom “supply chain“ útoku
  - Zlyháva riadenie dodávateľského reťazca a jeho bezpečnosť v každej/niektorej úrovni
  - Majiteľ infraštruktúry následne implementuje produkt zo zabudovaným útočným kódom vo viere, že je bezpečný

AKO JE TO TERAZ?

- Neriešením netechnických bezpečnostných povinností
  - organizácie kybernetickej bezpečnosti a informačnej bezpečnosti,
  - riadenia rizík kybernetickej bezpečnosti a informačnej bezpečnosti,
  - personálnej bezpečnosti,
  - riadenia prístupov,
  - riadenia kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahoch s tretími stranami,
  - akvizície, vývoja a údržby informačných sietí a informačných systémov,
  - kontinuity prevádzky,
  - auditu, riadenia súladu a kontrolných činností.

- A samozrejme personálnym poddimenzovaním
- a zanedbaným (chýbajúcim, slabým, formálnym) vzdelávaním všetkých zamestnancov

AKO JE TO TERAZ?

- Za bezpečnosť a odolnosť svojich produktov a služieb (a teda dát, ktoré spracovávajú) reálne **zodpovedajú firmy/organizácie samotné**
- Téma kybernetickej bezpečnosti sa z úrovne “IT oddelenie“ musí presunúť na úroveň „generálny riaditeľ/majiteľ/predstavenstvo“
- Štatutárny orgán organizácie, ktorá zlyhala v oblasti kybernetickej bezpečnosti môže byť trestne zodpovedný za svoje rozhodnutia (alebo nerozhodnutia)

AKO JE TO TERAZ?

- Celosvetová štatistika hovorí, že až 95% firiem robí (teda keď vôbec) kybernetickú bezpečnosť z dôvodu „compliance“ čiže zákonných povinností

- **Takže úlohou štátu dnes je**
  - Vysvetľovať, vysvetľovať, vysvetľovať
  - A popri tom vytvárať rozumné legislatívne požiadavky na kritické/kľúčové/dôležité subjekty tak, aby ich sa ich implementáciou položil zdravý základ riešenia kybernetickej bezpečnosti v organizácií
  - Zdieľanie best-practice informácii o incidentoch, útokoch, zraniteľnostiach
  - Analyzovanie zraniteľností a vytváranie všeobecných a adresných varovaní
  - Vytvárať atmosféru dôvery

AKO VYZERÁ PROSTREDIE, KDE SA TO ODOHRÁVA?

- Všetci sme zraniteľní voči počítačovej kriminalite
  - Zvyšujúci sa počet vlastných a pracovných zariadení
  - Digitalizácia nášho vlastného života
- Počítačová kriminalita je bežná
  - Pokus o hack každých 39 sekúnd, 4000 ransomware útokov denne len v USA
  - 87% firiem čelilo pokusu o zneužitie známej zraniteľnosti z internetu za rok
- Počítačová kriminalita je ekonomický problém
  - V 2021 globálne škody boli na úrovni 6 biliónov USD
  - Do 2025 globálny nedostatok odborníkov môže stáť 10 biliónov USD
- Počítačová kriminalita narúša osobné súkromie
  - Len Google v Jan/2021 registroval 2.145.013 phising webov
- Počítačová kriminalita je hrozbou pre národnú bezpečnosť
  - Kyber útoky majú priamy vplyv na ekonomiku a bezpečnosť štátov
- Miera počítačovej kriminality sa zvyšuje
  - Medziročný nárast v desiatkach percent

ĎAKUJEM

Rastislav Janota

rastislav.janota@nbu.gov.sk

NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

SK CERT