Zákon o kybernetickej bezpečnosti v IT systémoch

27. CESTÁRSKY DEŇ

Nie je možné chrániť a zabezpečiť to, čo nepoznáme.

Absolútna bezpečnosť neexistuje

SHIELD TECH, s.r.o.

SHIELD TECH

Poradenstvo pri projekčnej činnosti pri technológii v súlade so ZoKB

Analýza aktuálneho stavu kybernetickej bezpečnosti

Dokumentácia bezpečnostného projektu

Implementácia bezpečnostných riešení na kľúč

Penetračné testovanie

Analýza zraniteľnosti

Poskytovanie SOC služieb

Služba externého manažéra kybernetickej bezpečnosti

Prečo hovoríme o kybernetickej bezpečnosti

SHIELD TECH

80% všetkých európskych firiem zaznamenalo v roku 2017 aspoň **1 kybernetický incident**

V roku 2017 evidoval web Hackmageddon.com 868 veľkých **hacknutí a/alebo únikov dát.**

Len **24% spoločností** má vypracovaný plán týkajúci sa bezpečnostných incidentov, ktorý by im pomohol pri reakcii na kybernetický útok alebo incident spôsobený chybným správaním zamestnanca.

Štatistika slovenského CSIRT teamu za rok 2016 evidovala 1 613 156 bezpečnostných incidentov – iba ohlásených

85% útokov je vedených z interných systémov spoločnosti

Za implementáciu bezpečnostných opatrení je zodpovedný dozorný orgán spoločnosti prípadne konateľ spoločnosti

SHIELD TECH

Kybernetická bezpečnosť

Definícia siete a informačného systému v zmysle § 3 a) Zákona:

- elektronická komunikačná sieť, informačný systém, každé zariadenie a komunikačný systém alebo údaj, ktoré sú v nich vytvárané, ukladané, spracúvané, získavané alebo prenášané prostredníctvom elektronickej komunikačnej siete alebo informačného systému, na účely prevádzkovania, používania, ochrany a udržiavania týchto sietí a systémov.

Definícia kybernetickej bezpečnosti v zmysle § 3 g) Zákona:

- Stav, v ktorom sú siete a informačné systémy schopné odolávať na určitom stupni spoľahlivosti akémukoľvek konaniu, ktoré ohrozuje dostupnosť, pravosť, integritu, alebo dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov alebo súvisiacich služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a informačných systémov

SHIELD TECH

Čo to je?

Kybernetická bezpečnosť je spojením

Aplikačnej bezpečnosti

Informačnej bezpečnosti

Network bezpečnosti

BCM a disaster recovery

Operačnej bezpečnosti (OPSEC)

End-user vzdelávania

Cieľom kybernetickej bezpečnosti nie je mať všetky existujúce security nástroje

avšak účinne využívať relevantné nástroje, ktoré sú už k dispozícii prípadne vhodne doplniť chýbajúce na zaistenie ochrany

SHIELD TECH

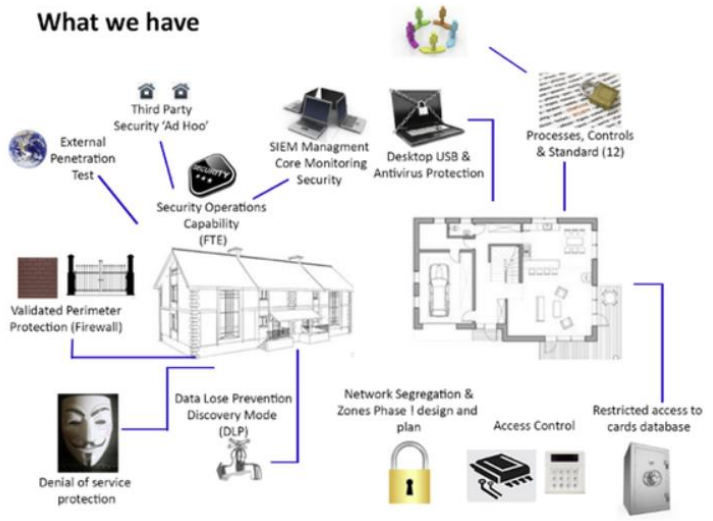
Ako na to ?

SHIELD TECH

1. Analýza aktuálneho stavu informačných a OT systémov (GAP analýza)

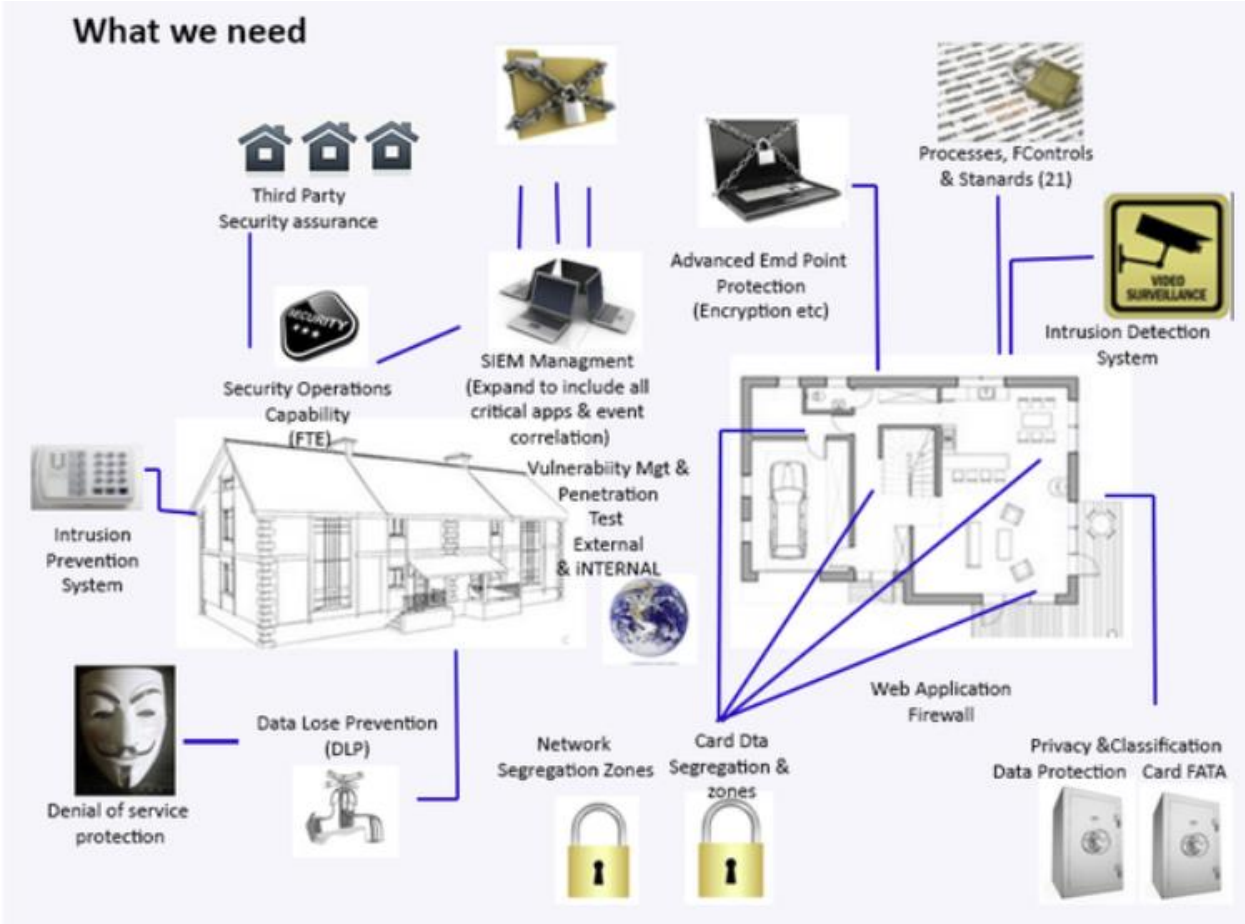
2. Vytvorenie procesného modelu organizácie a definovanie aktív a systémov

3. Analýza rizík a analýza dopadov s pridanou hodnotou



SHIELD TECH

Nie je možné a nemali by sme žiadať, aby boli všetky riziká okamžite vyriešené. Je potrebné prijať prístup založený na riziku a prijať opatrenia, ktoré riešia najväčšie riziká pre domácnosť (spoločnosť) okamžite a tým si vytvoríme priestor pre časový plán na mitigáciu ostatných rizík podľa ich priority.



SHIELD TECH

4. Riadenie kontinuity činnosti (BCM)

5. Security Operations Centre (SOC)

6. Computer Security Incident Response Teams (CSIRT)

SHIELD TECH

7. Vzdelávanie zamestnancov

- Školenia zamerané na cybersecurity
- Príprava legislatívnych školení (GDPR, ZoKB, DPO...) so zameraním na všetky úrovne organizácií
- Školenia spojené s certifikáciou ISO 27000, hlavne pre pozíciu audítora
- Workshopy pre verejný a komerčný sektor podľa aktuálnych tém buď legislatívnych (GDPR. ZKB, NIS, atď.)

SHIELD TECH

Trocha teórie

SHIELD TECH

Bezpečnosť informácií

Organizácia	Technologické prostredie
Ochrana údajov	Klasifikácia informácií
Riadenie IT rizík	Manažment zrnaniteľností
Havarijné plánovanie	Security Governance
IT architektúra	Riadenie aktív
Riadenie prístupov	Riadenie zmien a konfigurácií
Riešenie incidentov	Service Level Management
Vzťahy a komunikácia	Biznis architektúra
Ekosystém partnerov	Vzdelávanie a povedomie

Základné atribúty spoľahlivosti informácie

SHIELD TECH

Confidentiality (Dôvernosť):

- miera obmedzenia prístupu k informáciám len pre osoby, alebo skupiny osôb, ktoré sú oprávnené na prístup k príslušným informáciám.

- **Privacy (ochrana súkromia):**
- ochrana pred nežiadanou publicitou, verejnou kontrolou, sledovaním alebo neoprávneným zverejnením osobných údajov

Integrity (Celistvosť)

- miera bezchybnosti a informácie
- Charakteristikami integrity sú:
  - Úplnosť informácie
  - Správnosť informácie

Availability (Dostupnosť)

- miera dostupnosti informácie pre používateľa a systém vo chvíli, keď je informácia potrebná a požadovaná

SHIELD TECH

Opatrenie

Ochranné (bezpečnostné) opatrenia: (angl.: measures, controls):

- Sú **praktiky, procedúry a mechanizmy**, ktoré môžu pomôcť chrániť pred nejakou hrozbou, znížiť zraniteľnosť, obmedziť vplyv nechcenej udalosti, odhaliť malígnu udalosť a umožniť zotavenie alebo odškodnenie

Opatrenie na účely zákona v zmysle §20 (1) Zákona:

- **Úlohy, procesy, role a technológie** v organizačnej, personálnej a technickej oblasti, ktorých cieľom je zabezpečenie kybernetickej bezpečnosti počas životného cyklu sietí a informačných systémov.

Generické rozdelenie bezpečnostných opatrení

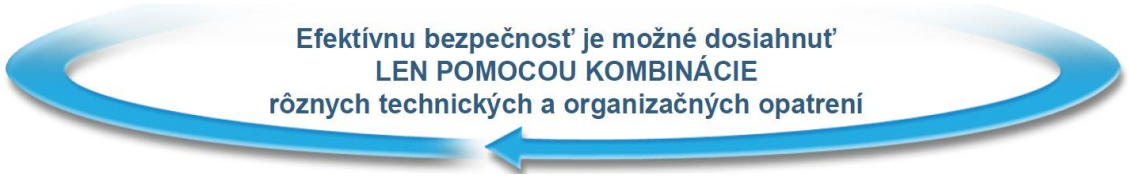
SHIELD TECH

Technické opatrenia

- Opatrenia na zníženie bezpečnostných rizík pomocou prostriedkov a fyzickej a technologickej povahy

Organizačné opatrenia

- Opatrenia na zníženie bezpečnostných rizík pomocou zmien procesov a úpravou dokumentácie
- **Personálne opatrenia**
  - Podkategória organizačných opatrení týkajúcich sa riadenia ľudských zdrojov



Rozdelenie bezpečnostných opatrení podľa ZoKB

SHIELD TECH

§ 19 (1) Prevádzkovateľ základnej služby je povinný do šiestich mesiacov odo dňa oznámenia o zaradení do registra prevádzkovateľov základných služieb prijať a dodržiavať:

- **Všeobecné bezpečnostné opatrenia** najmenej v rozsahu bezpečnostných opatrení podľa §20
- **Sektorové bezpečnostné opatrenia**, ak sú prijaté

Podrobnosti:

- Vyhlášku č. 362/2018 Z.z. NBÚ, ktorou sa stanoví obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení

SHIELD TECH

Bezpečnostné opatrenia

§ 20 (3) Bezpečnostné opatrenia sa prijímajú najmä pre oblasť:

a) Organizácie informačnej bezpečnosti
b) Riadenia aktív, hrozieb a rizík
c) Personálnej bezpečnosti
d) Riadenia dodávateľských služieb, akvizície, vývoja a údržby informačných systémov
e) Technických zraniteľností systémov a zariadení
f) Riadenia bezpečnosti sietí a informačných systémov
g) Riadenia prevádzky
h) Riadenia prístupov
i) Kryptografických opatrení
j) Riešenia kybernetických bezpečnostných incidentov
k) Monitorovania, testovania bezpečnosti a bezpečnostných auditov
l) Fyzickej bezpečnosti a bezpečnosti prostredia
m) Riadenia kontinuity procesov

Minimálny rozsah bezpečnostných opatrení

SHIELD TECH

§ 20 (4) Bezpečnostné opatrenia musia zahŕňať najmenej:

a) Detekciu kybernetických bezpečnostných incidentov

b) Evidenciu kybernetických bezpečnostných incidentov

c) Postup riešenia a riešenie kybernetických bezpečnostných incidentov

d) Určenie kontaktnej osoby pre prijímanie a evidenciu hlásení

e) Pripojenie do komunikačného systému pre hlásenie a riešenie kybernetických bezpečnostných incidentov a centrálneho systému
včasného varovania

SHIELD TECH

Kybernetická bezpečnosť nie je Váš problém, je to naša starosť, aby ste mali čas rásť.

25. 11. 2020

SHIELD TECH

ĎAKUJEM ZA VAŠU POZORNOSŤ