SLOVENSKO ZAVAROVALNO ZDRUŽENJE
Slovenian Insurance Association

Kibernetska tveganja v transportu

Margita Selan Voglar

Nove tehnologije in povezana vprašanja

1. Internet stvari – pametni kontejnerji (Smart containers), pametna logistika (Smart logistics)
2. E-navigacija
3. Kibernetski riziki
4. Zavarovanje

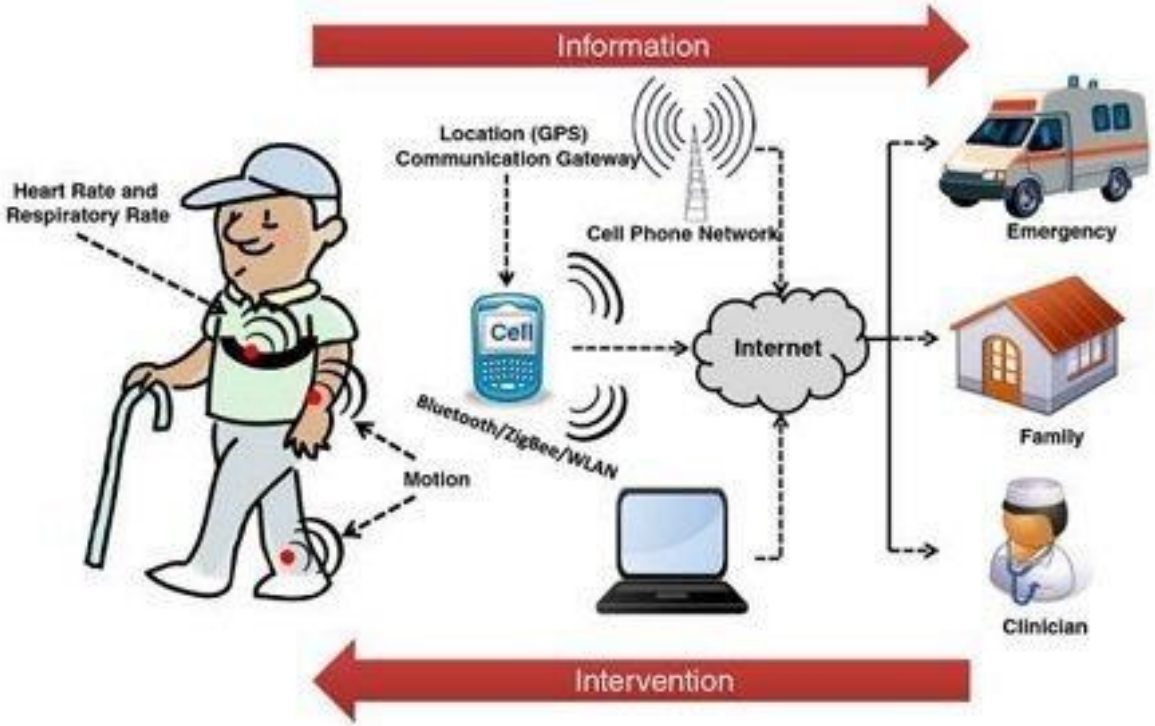
Internet stvari (IoT)

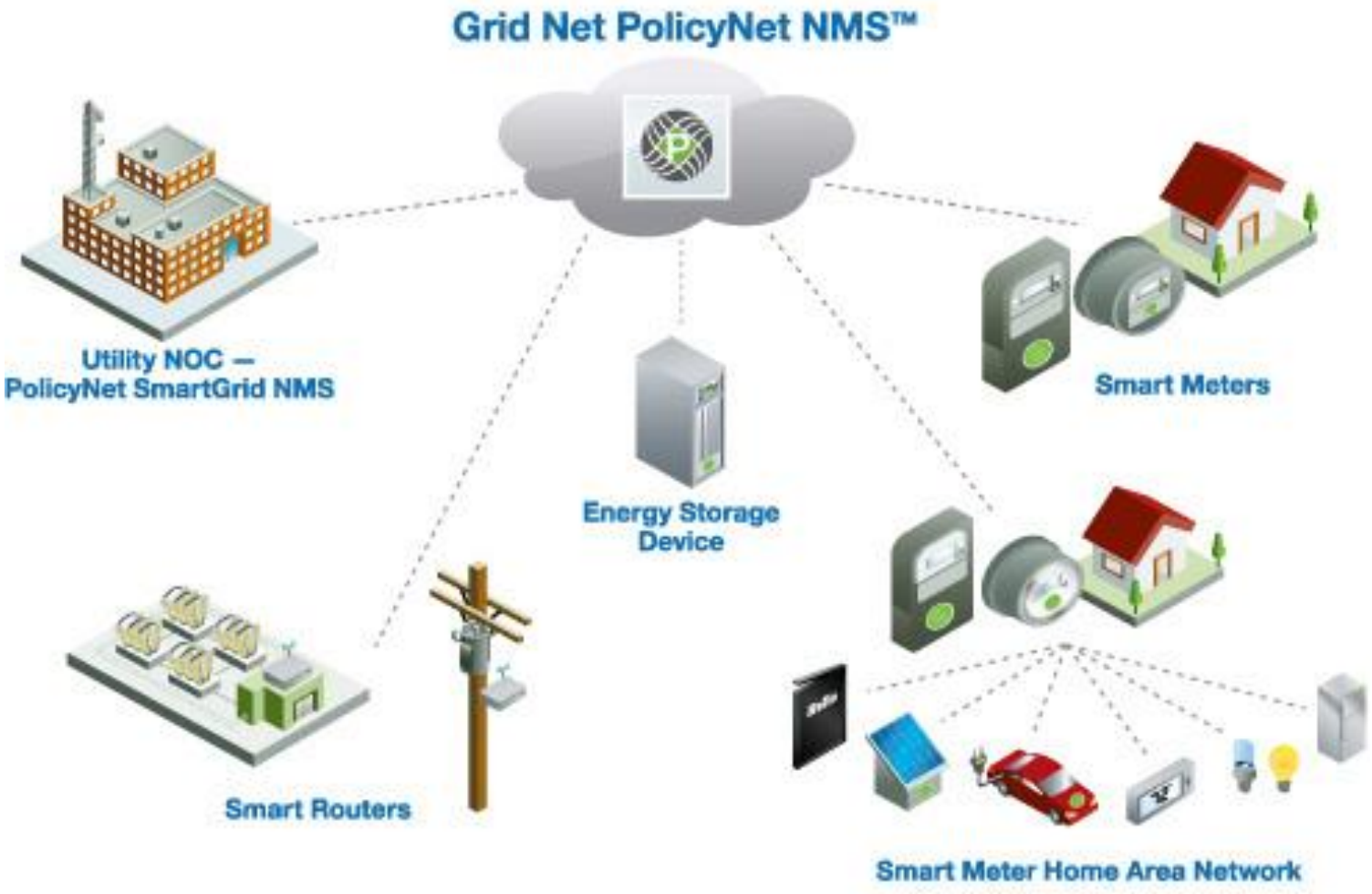
Internet stvari ali medomrežje stvari - proces povezovanja velike količine naprav, ki imajo vgrajene tipala/senzorje, ki bolj ali manj samostojno komunicirajo med seboj in prek najrazličnejših aplikacij izmenjujejo podatke. Te naprave so lahko aparati bele tehnike doma, avtomobili in druga prevozna sredstva ali pa na primer stroji v proizvodnji. IoT omogoča, da so predmeti zaznani ali vodeni na daljavo preko obstoječe medmrežne infrastrukture ter omogoča možnosti za neposredno integracijo fizičnega sveta v računalniški sistem ter rezultira v izboljšani učinkovitosti, natančnosti in ekonomskih učinkih kot dodatek k zmanjšani človeški vpletenosti / intervenciji v poslovanje. (vir:Wikipedija).

IoT zajema tri vrste komunikacije

1. *Komunikacija naprav z ljudmi,*
2. *Komunikacija med napravami,*
3. *Komunikacija med stroji (machine to machine M2M)*

Telemedicine




Grid Net PolicyNet NMS™
Utility NOC —
PolicyNet SmartGrid NMS
Smart Meters
Energy Storage
Device
Smart Routers
Smart Meter Home Area Network

Smart Port Logistics powered by

IoT prodira v vse pore življenja in poslovanja. Zbiranje podatkov s pomočjo različnih naprav in obstoječih tehnologij ter avtonomen pretok podatkov z drugimi napravami poznan kot npr. „Smart home“, „Smart cities“, „Apple watch“…

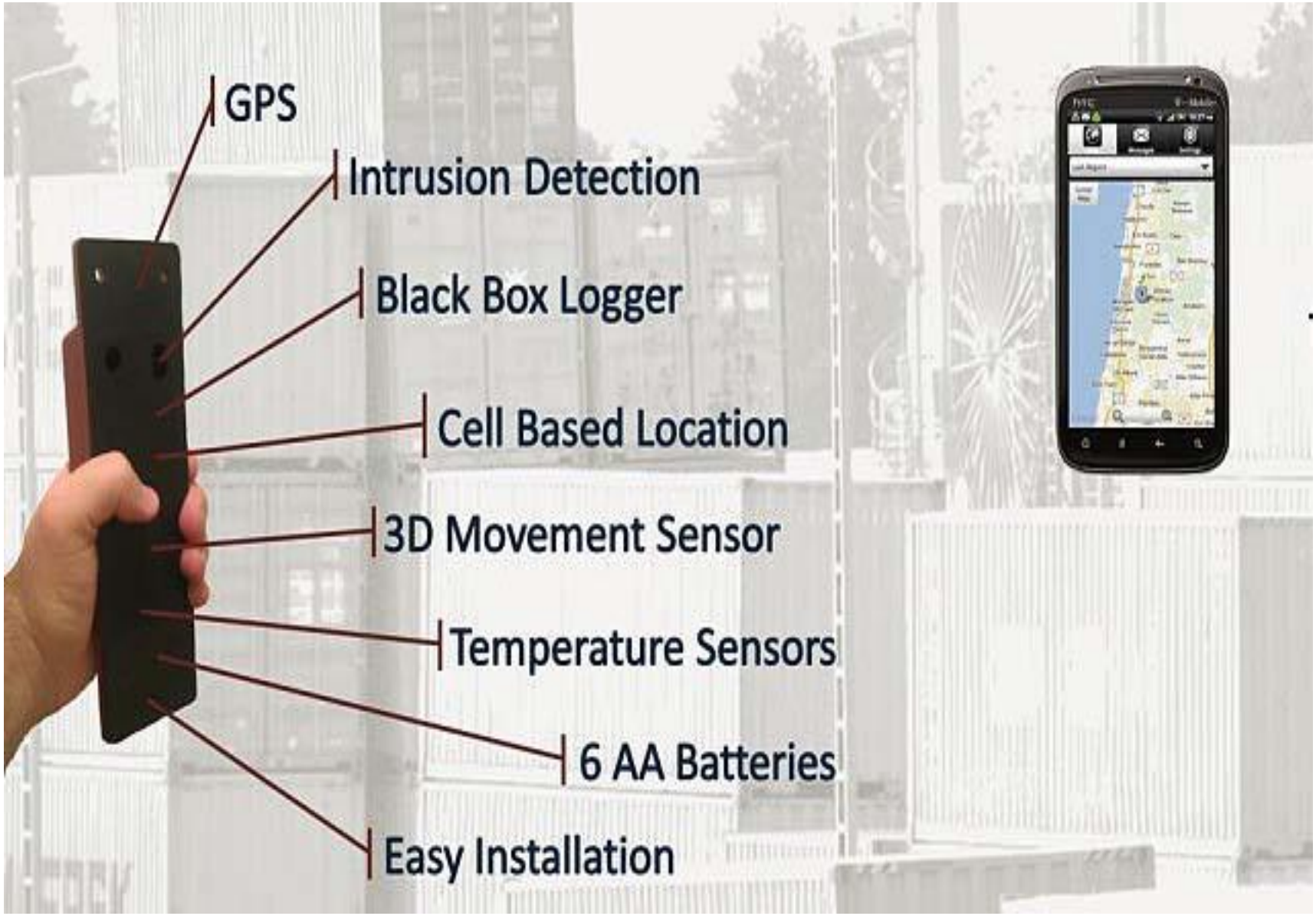
Količina zbranih podatkov terja njihovo hitro varovanje, urejanje in hrambo (v oblaku).

Smart logistics – avtomatizacija tradicionalnih oskrbovalnih verig

Naprave omogočajo nadzor tovora in postopkov v zvezi s tovorom:

1. *Ugotavljanje trenutne lokacije tovora, premiki (dovoljeni in nedovoljeni), morebitne deviacije iz začrtane poti,*
2. *Stanje tovora – temperatura, vlaga, osvetljenost, tlak,*
3. *Tresljaji katerim je tovor podvržen v času potovanja,*
4. *Zamude tovora na poti,*
5. *Posegi v tovor (nepravilno rokovanje) – možnost alarmiranja,*
6. *Realni podatki o stanju tovora v skladišču in lažje prilagajanje zavarovalnih kritij premij.*

Pametna logistika omogoča, da se težave/nepravilnosti/dogodki zaznajo še pred nastankom škode, kar omogoča zgodnje ukrepanje – npr. ogled tovora še pred prispetjem v namembni kraj, izvajanje ukrepov za zmanjšanje škode, povrnitev morebitno odtujenega tovora; lažja subrogacija, ker se ve, kje je škoda nastala.


GPS
Intrusion Detection
Black Box Logger
Cell Based Location
3D Movement Sensor
Temperature Sensors
6 AA Batteries
Easy Installation

1. Batteries In

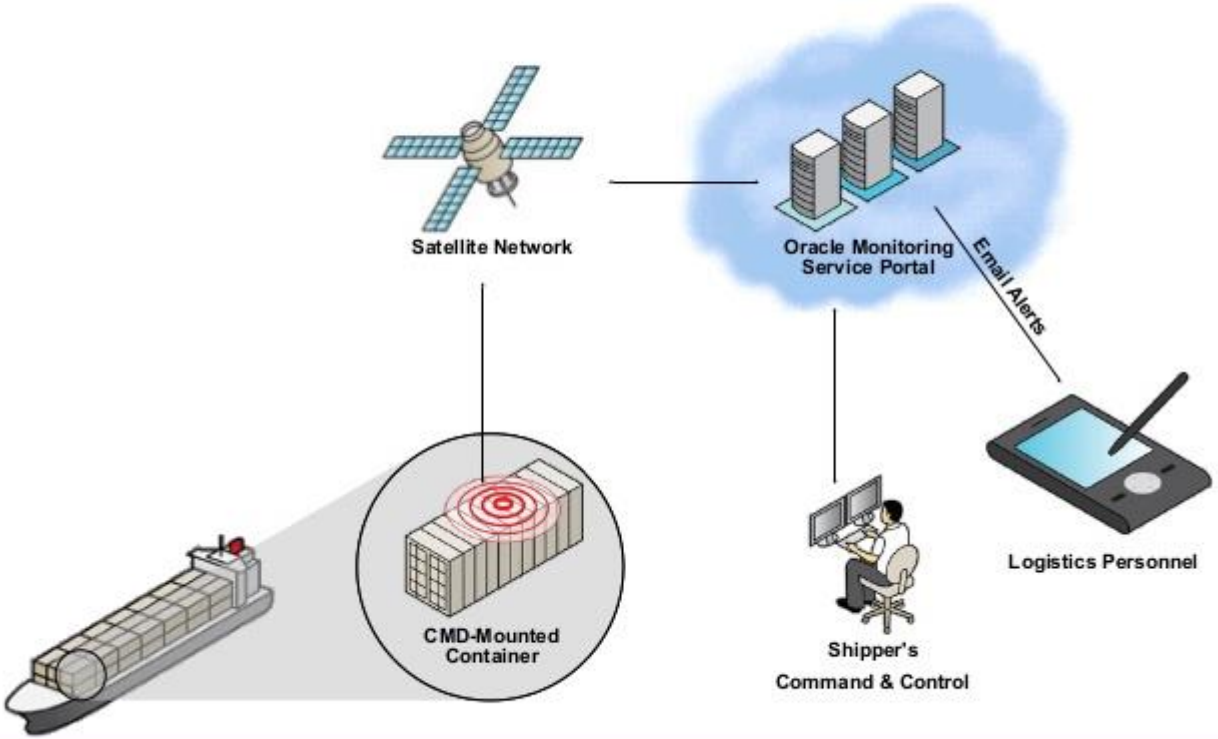
2. Attach

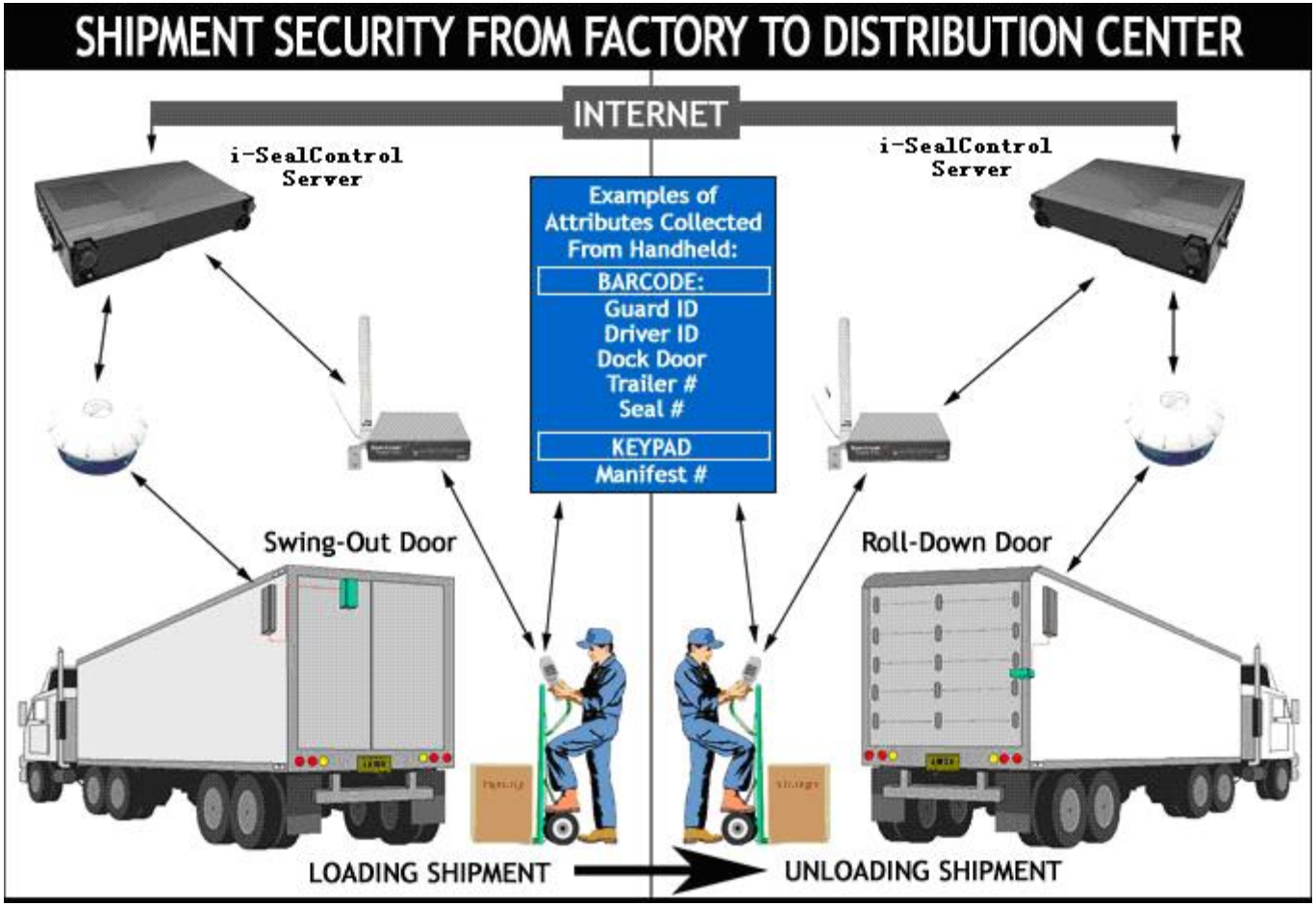
3. Ready!

Looks and installs exactly like a normal container vent

Invisible when attached to a shipping container!

Smart Container Solution Architecture




SHIPMENT SECURITY FROM FACTORY TO DISTRIBUTION CENTER
INTERNET
i-SealControl Server
i-SealControl Server
Examples of Attributes Collected From Handheld:
BARCODE:
Guard ID
Driver ID
Dock Door
Trailer #
Seal #
KEYPAD
Manifest #
Swing-Out Door
Roll-Down Door
LOADING SHIPMENT
UNLOADING SHIPMENT

E- navigacija

IMO definicija:

Usklajeno zbiranje, vključevanje, izmenjava, predložitev in analiza pomorskih informacij z elektronskimi sredstvi na krovu ladje ali na kopnem z namenom izboljšanja navigacije od sidrišča do sidrišča in povezanih storitev za varnost in varovanje na morju ter zaščita morskega okolja. (vir: Wikipedija)

E-navigacija pomeni precizno definirano strategijo vključevanja novih in obstoječih orodij za navigacijo za izboljševanje uporabe in varnosti ladij na morju.

Pomorska industrija je v preteklih obdobjih doživela serijo tehnoloških napredkov. Kot drugod je tudi v tem segmentu prišlo do množične digitalizacije ladijskih motorjev in opreme. Moderne ladje uporabljajo digitalno opremo – AIS (Automatic identification system), ECDIS (Electronic chart disply and information system), Integrated Bridge Systems, Automatic Radar Plotting Aids, Long Range Identification and Tracking, GMDSS in ostala moderna elektronska orodja za navigacijo.

Cilj e-navigacije je razvitje sistema, ki bo na primeren in pravilen način organiziral vse podatke o ladji na enem mestu, da bi omogočil izboljšanje navigacijske varnosti ladij.

Kompleksnost ITC (Information, Technology and Communication) z uporabo posebnih tehnologij terja zagotavljanje primernih varnostnih postopkov v pomorskih sistemih. Opozorila in iniciative po ureditvi ne le fizičnih aspektov varnosti in varovanja, pač pa tudi kibernetičnih, se je pojavila že v preteklem desetletju.

Avtonomne ladje – fikcija ali realnost?

Nevarnosti:

- *Zanašanje na tehnologijo, pomanjkljivo šolanje posadke, premajhno število članov posadke, prevelika obremenjenost ljudi,*
- *Hekerji z vdori v podjetja vnašajo negotovost in škodo družbam,*
- *Povečuje se število poročil o incidentih, ko je moten GPS na morjih – spoofing napadi, ko se ladjo „spelje“ s planirane poti in povzroči nasedanje, trčenje ali podobni pomorski incidenti,*
- *Povezanost mnogih različnih sistemov v navigaciji še povečuje ranljivost zaradi potrebe po odprtosti in medsebojni komunikaciji različnih sistemov in komponent (različni proizvajalci),*
- *Nepridipravi izkoriščajo vrzeli in napadajo – kraja podatkov, motenje signalov, zavajanje, kraja tovora, izsiljevanje, premoženjska škoda, poškodbe ljudi ali izgube življenj, katastrofe – okoljske,*
- *Pred napadi niso varna niti pristanišča.*

Ukrepi

1.6.2016 je IMO izdal cirkularno pismo MSC.1/Cir.1526 z začasnimi/vmesnimi navodili o upravljanju pomorskih kibernetskih rizikov.

V juliju letošnjega leta so bila izdana Navodila za upravljanje pomorskih kibernetičnih nevarnosti s strani IMO – potreba po povečanju zavedanja o nevarnostih in ranljivosti ladijske plovbe pred kibernetskimi napadi.

Navodila vsebujejo priporočila in ukrepe za zaščito pred kibernetičnimi nevarnostmi, katerim je izpostavljena tehnologija plovbe in ki ogrožajo delovanje, varnost in varovanje ladje v primeru, če bi bil sistem napaden, izgubljen ali poškodovan.

Cyber risk – kibernetični riziki

1. *Zbiranje, beleženje, obdelava podatkov in varna hramba v oblaku – tarča vdorov in kraje oz. nepooblaščene uporabe podatkov,*
2. *Naprave za sledenje, ki sporočajo natančno lokacijo – zaklad informacij za nepridiprave,*
3. *Vdori v podatke, ki so dolgo ne zaznani,*
4. *Delovanje litij-ionskih baterij in njihova omejenost trajanja,*
5. *Riziko kontaminacije z virusi,*
6. *Hektivizem,*
7. *Terorizem.*

- *IoT aplikacije? Lažen občutek varnosti*

Situacija na trgu kibernetičnih zavarovanj

- *Skupna, obračunana premija je v strmi rasti – (ZDA 4 mrd USD v 2016, 3,2 mrd USD v 2015),*
- *Premije se pri obnovah zavarovanj znižujejo od 10 do 20%, franšize se znižujejo,*
- *Velik interes za zavarovanje kažejo mala in srednja podjetja – močno prisotna zavest zaradi odgovornosti glede posesti osebnih podatkov,*
- *Produkti so različni, prilagojeni različnim industrijam – npr. bančništvo in finančne institucije, kartično poslovanje, zdravstvo, izobraževanje, javna uprava ipd.,*
- *Pokrivajo ali lastno škodo ali škodo povzročeno tretjim,*
- *Ni pa pokrita vsa nastala škoda – izguba intelektualne lastnine, telesne poškodbe, okvare zdravja ali smrt, premoženjska škoda, škoda ugledu, izpad dohodka…,*

Kibernetična kritja v transportnih zavarovanjih

- *Večina domačih in mednarodnih zavarovalnih pogojev za zavarovanje transportnih nevarnosti vsebuje „Cyber Attack Exclusion Clause (CL380) 10/11/2003“, ki izključuje kakršnokoli izgubo, poškodbo ali odgovornost povzročeno neposredno ali posredno z uporabo računalnika in z njim povezanih sistemov in softwara kot sredstev za povzročitev škode.*
- *Potrebe po kritju so velike, zavarovatelji ugotavljajo potencialne obsege škode, ki bi jih strankam povzročili kibernetični vdori, da oblikujejo kritja potrebna za zaščito ladij in pomorskih družb,*
- *Ocena rizika in izpostavljenosti ter potenciala vpliva na premijo.*

Kritja za kibernetične nevarnosti

Obstajajo tri osnovna kritja

- *Odgovornost za izgubo ali vdor v podatke – zaščita zavarovanca, če bi bil tožen, da je do vdora prišlo zaradi malomarnega varovanja podatkov,*
- *Kritje stroškov reakcije odpravljanja posledic vdora – kriznega managmenta– krijejo stroške preiskave, PR, obveščanja strank in spremljanje kreditnega tveganja,*
- *Kritje glob in kazni predpisani z zakonom ali predpisi – kriti so stroški preiskave, obrambe ter plačila glog in kazni. Večina zavarovateljev tega kritja ne nudi!*
- *PCI (kreditne kartice) globe in kazni – vključuje stroške forenzične preiskave in ponovne izdaje kartic.*

Sprožilci jamstva

- *Opustitev varovanja podatkov,*
- *Izguba, ki jo povzroči zaposleni,*
- *Dejanja oseb, ki niso zavarovanec,*
- *Izguba, ki izvira iz tatvine ali izginotja osebnega premoženja (npr. podatki na ukradenem prenosniku)*

Stroški odgovora na vdor

- *Gotovo je kritje teh stroškov najpomembnejši del jamstva – krije stroške odziva na vdor v podatke (obveščanje strank, zmanjševanje negativnega vpliva na ugled in analizo kreditnega tveganja - vse to so visoki stroški),*
- *Postopek je lahko v naprej definiran, kar olajšuje situacijo – uporabljajo se storitve zunanjih ponudnikov, ki so lahko že v naprej dogovorjeni in trajanje njihovih storitev.*

Zahteve glede varnostnih ocene rizika za zavarovanje

- *V začetku je bilo to obvezno pred sklenitvijo zavarovanj kibernetičnih nevarnosti,*
- *Klientu so strokovnjaki po pregledu dali informacije glede ranljivosti in pomanjkljivosti, ki jih mora odpraviti ali spremeniti,*
- *Če so bili kriteriji doseženi, je vplivalo na ugodnejšo premijo.*

Kritje kibernetičnih nevarnosti v transportu

- *Gotovo bo na trgu kmalu produkt za kritje ladij in pristaniščč,*
- *Zavarovanje rizika na pametnih kontejnerjih bi bil lahko testni primer?*

Kaj stranke še potrebujejo?

- *Škoda zaradi telesne poškodbe ali premoženjska škoda s cyber policami niso krite,*
- *Škoda zaradi tatvine intelektualne lastnine ni krita,*
- *Kritje za odgovornost zaradi medijskih prestopkov, obrekovanja*

Hvala za pozornost!