SEKCIJA ZA KIBERNETSKO VARNOST

ZIT
Združenje za informatiko in telekomunikacije

Gospodarska zbornica Slovenije

Zakonodaja na področju informacijske varnosti prinaša nove zahteve za izvajalce zdravstvenih storitev

Marko Zavadlav

20.11.2017

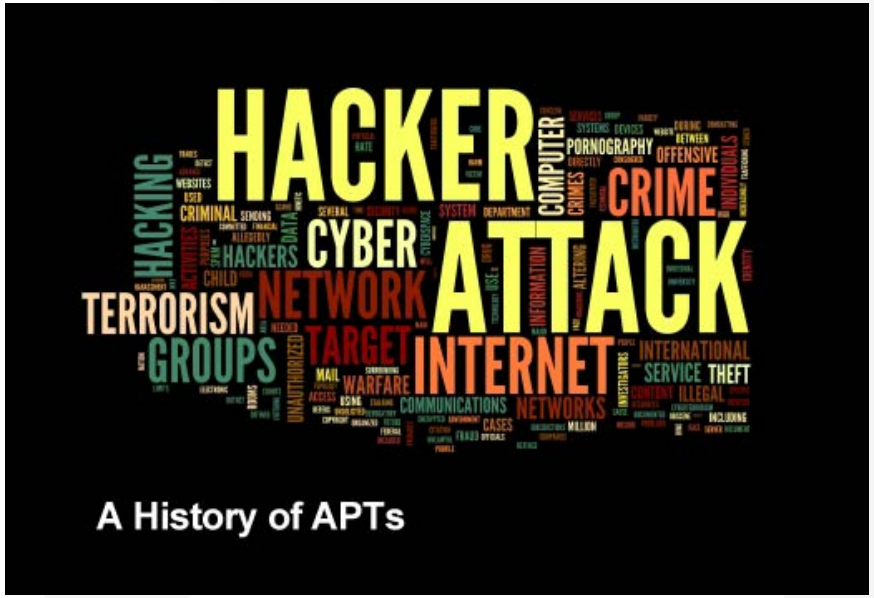
- Vsi govorimo o splošni uredbi o varstvu podatkov GDPR
- Kaj pa NIS? DIREKTIVA (EU) 2016/1148 EVROPSKEGA PARLAMENTA IN SVETA z dne 6. julija 2016 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji

Sekcija za Kibernetsko Varnost

- Kaj je NIS in kaj je Zakon o informacijski varnosti?
- Kakšne spremembe prinaša in za koga?
- izzivi!
- Pristop
- Q&A

Direktiva NIS in Zakon o informacijski varnosti

- Direktiva NIS je bila sprejeta 6.7.2016, v zakonodajo mora biti prenesena maja 2018 (9.11.2018 določitev izvajalcev bistvenih storitev)
- Opredeljuje ukrepe za zagotavljanje visoke ravni varnosti omrežij in informacijskih sistemov pri izvajalcih bistvenih storitev
- Določi izvajalce bistvenih storitev
- Določi obveznosti izvajalcev bistvenih storitev
- Določi obveznosti države članice



Bistvene storitve (4. člen)

Zavezanci, ki so izvajalci bistvenih storitev zagotavljajo dele omrežja oziroma delujejo v naslednjih sektorjih:

- energija,
- digitalna infrastruktura,
- oskrba s pitno vodo in njena distribucija,
- zdravstvo,
- promet,
- bančništvo,
- infrastruktura finančnega trga.

Merila iz ZIV

Osnovna merila za določitev zavezancev, ki so izvajalci bistvenih storitev so:

- subjekt zagotavlja storitev, ki je bistvena za ohranitev ključnih družbenih in/ali gospodarskih dejavnosti iz 2. odstavka 4. člena,
- zagotavljanje te storitve je odvisno od omrežij in informacijskih sistemov,
- incident bi imel pomemben negativen vpliv na nemoteno zagotavljanje te storitve,
- skrb za najmanj 5.000 prebivalcev Republike Slovenije ali delovanje na geografskem območju, večjem od 1% ozemlja Republike Slovenije.

Obveznosti zavezancev in naloge vodje informacijske varnosti

- Zavezanci skladno z dejavnostjo, ki jo opravljajo ter metodologijo, predpisano s posebnim predpisom, prepoznajo ključne, krmilne in nadzorne informacijske sisteme in dele omrežja, s katerimi zagotavljajo izvajanje storitev opredeljenih v 4. členu.
- Zavezanci iz 4. člena morajo imeti na svojih pripoznanih ključnih, krmilnih in nadzornih sistemih vzpostavljena in redno posodabljana orodja in mehanizme za zaznavanje incidentov ali morebitnih kibernetskih napadov, o čemer morajo voditi tudi zapise v dokumentaciji o posegih.

Organizacijski, logično-tehnični in tehnični ukrepi
Organizacijski ukrepi

- opredelitev varnostnih zahtev za dobavitelje,
- upravljanje sredstev,
- zagotavljanje visoke ravni integritete človeških virov,
- upravljanje prometa in komunikacij,
- dokumentiran razvoj in vzdrževanje informacijskih sistemov ,
- obvladovanje incidentov.

Organizacijski, logično-tehnični in tehnični ukrepi
Logično-tehnični ukrepi

- zagotavljanje fizičnega in tehničnega varovanja dostopov do prostorov, kjer se nahajajo ključni, krmilni ali nadzorni informacijski sistemi zavezanca,
- zagotavljanje mehanizmov za varnost v posamezni aplikativni podpori za izvajanje dejavnosti zavezanca
- uporaba orodij za zbiranje in vrednotenje incidentov.

Organizacijski, logično-tehnični in tehnični ukrepi
Tehnični ukrepi

- uporaba orodij za zaščito celovitosti komunikacijskih omrežij,
- uporaba orodij za preverjanje identitete uporabnikov,
- uporaba orodij za upravljanje pooblastil za dostop,
- uporaba orodij za zaščito pred zlonamernimi kodami,
- uporaba orodje za beleženje dejavnosti kritične informacijske infrastrukture in pomembnih informacijskih sistemov, njihovih uporabnikov in administratorjev,
- uporaba orodij za zaznavanje incidentov,
- uporaba akreditiranih šifrirnih mehanizmov in
- uporaba orodij za zagotavljanje ravni dostopnosti informacij.

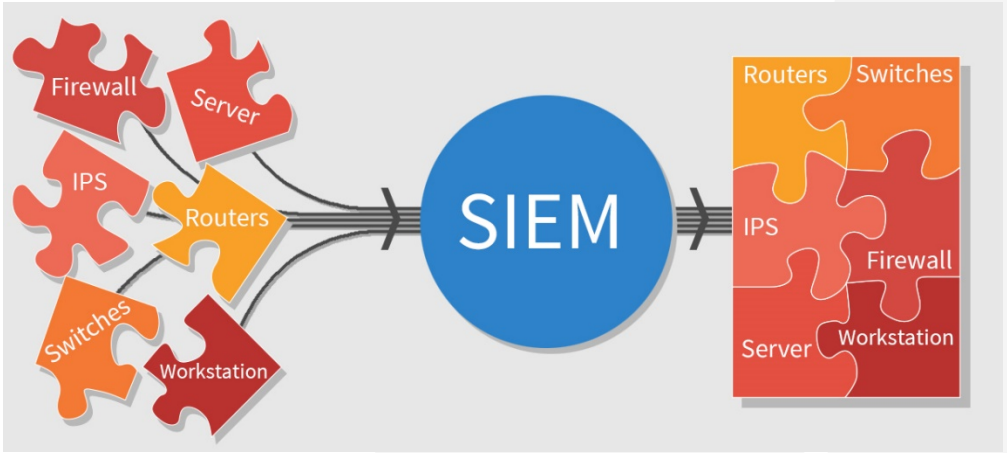
PRISTOP K ORGANIZACIJSKIM UKREPOM

SUVI

- Analiza tveganja
- Analiza vpliva na poslovanje
- Katalog IKT storitev
- Popis IKT virov, ki podpirajo kritične storitve
- Organizacijska shema s pooblastili
- Načrt neprekinjenosti poslovanja
- IKT procesi (odzivi na varnostne incidente)

PRISTOP K LOGIČNO-TEHNIČNIM UKREPOM

Orodja za zbiranje in vrednotenje incidentov, upravljanje varnostnih incidentov in dogodkov



- SIEM
- SIAMaaS (upravljana storitev)
- SOC (proaktivno in reaktivno delovanje)
- SOCaaS (upravljana storitev)
- Sistemi za upravljanje dogodkov, incidentov ter poročanje

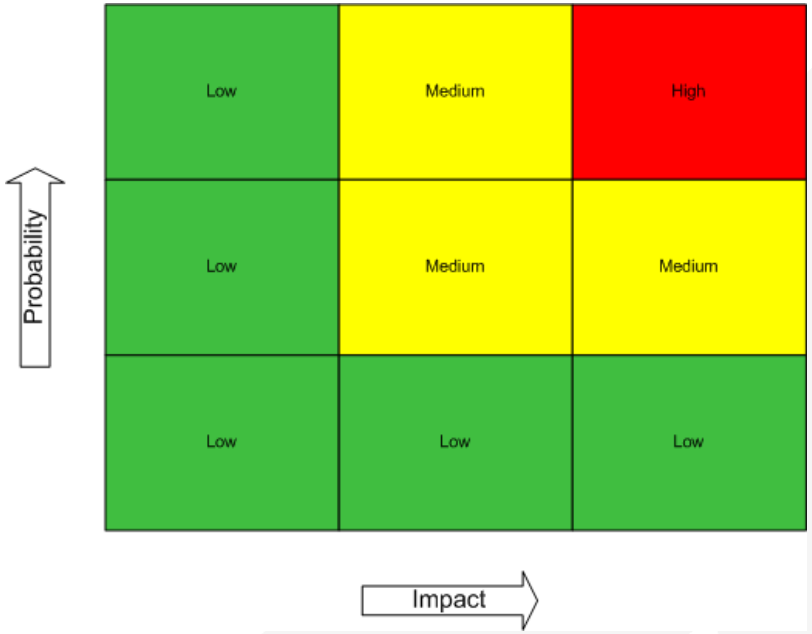
PRISTOP K TEHNIČNIM UKREPOM

Tehnične varnostne rešitve

- NGFW
- Antivirus
- APT
- DLP
- SIEM (revizijske sledi, beleženje dogodkov, korelacije, alarmiranje)
- IDS/IPS
- IAG (Identity, Access, Privileged Account Governance)

KLJUČNI DEJAVNIKI USPEHA

- Postopnost
- Natančnost
- Izobraževanje in ozaveščanje
- Vidnost
- Sodelovanje in izmenjava informacij



Sekcija za Kibernetsko Varnost

?

marko.zavadlav@unistarpro.si

PRO.astec