Kibernoziegumi

1. Preventīvie pasākumi

Apdraudējuma identifikācija
Valsts un pašvaldības iestāžu, kritiskās infrastruktūras un saimnieciskās darbības objektu darbības daļēja vai pilnīga paralizēšana.

Vēsturiskie dati
No 2004.gada tiek regulāri fiksēti uzbrukumi valsts iestāžu, pašvaldību un uzņēmumu mājas lapām un elektroniskajām sistēmām
2017. gadā nepārtikas veikalu ķēdēm
2017. gads e-veselībai un VID sistēmām
2018. gads globāls kiberuzbrukums ES valstīm un ASV
2021. gads uzbrukums maģistrālajam naftas vada operatoram “Colonial Pipeline” ASV
2021. gads hakeru uzbrukums ASV IT kompānijai ‘Kaseya” varētu būt ietekmējis līdz pat 1500 uzņēmumiem visā pasaulē.

Prognozējamība
Risks nav prognozējams

Riska līmenis
Zems risks (iespējams ar pavisam nenozīmīgām sekām)

Riska samazināšanas pasākumi
Nav nepieciešami

Riska uzraudzība
Kirernoziedznieku aktivitāšu uzraudzība

Riska ziņošana
Valsts policijas pārstāvis fiksē kibernoziegumu gadījumus un ziņo ikgadējā CAK sanāksmē par risku pārvaldību

Nepieciešamie resursi riska pārvaldībai

- Speciāli resursi nav nepieciešami

2. Gatavības pasākumi

Gatavības pasākumus nodrošina par risku atbildīgie valsts un pašvaldību dienesti un institūcijas.

3. Reaģēšanas rīcību algoritmi

Zemiem riskiem reaģēšanas rīcību algoritmi netiek izstrādāti. Reaģēšanas rīcības tiks organizētas atbilstoši situācijai.