Kiberdrošība publiskajā pārvaldē – darbinieku loma un atbildība

Kiberdrošība publiskajā pārvaldē – darbinieku loma un atbildība ir 20 akadēmisko mācību stundu kurss publiskajā pārvaldē nodarbinātajiem komandu vadītājiem. Tās tiks organizētas kā praktiski semināri vienas organizācijas vai resora grupām, ar iespēju apvienot līdzīgus amatu līmeņus (10–20 dalībniekiem). Saturs tiks pielāgots konkrētajai iestādei. Mācību mērķis – stiprināt vadītāju zināšanas un prasmes kiberdrošības risku vadībā, veidot drošu digitālo vidi un atbildīgu kiberdrošības kultūru publiskajā pārvaldē.

Formāts

Mācību norises laiks ir paredzēts darba dienās. Atsevišķi vienojoties mācības var tikt organizētas arī brīvdienās

Formāts:

- Attālināti tiešsaistes platformā ZOOM.
- Klātienē Valsts administrācijas skolā, Rīgā, Raiņa bulvārī 4 vai pēc savstarpējās vienošanās mācībās iesaistīto organizāciju telpās (tehnisko aprīkojumu nodrošina organizācija, kurā notiek mācības), vai Ventspils Augsto tehnoloģiju parka, Ventspils Augsto tehnoloģiju parks 1 telpās.

Programmas mērķis

Mācību mērķis ir nodrošināt publiskajā pārvaldē nodarbinātajiem komandu vadītājiem praktiskas zināšanas un izpratni par kiberdrošības risku vadību, lai veidotu drošāku digitālo vidi organizācijā, stiprinātu kiberdrošības kultūru un spēju pieņemt lēmumus attiecībā uz organizācijas digitālo aizsardzību.

Kāpēc piedalīties?

Iegūsi skaidru priekšstatu par kiberdrošības nozīmi publiskajā pārvaldē un savām atbildībām, izpratīsi aktuālos draudus un to ietekmi uz iestādes darbību, apgūsi normatīvo prasību izpildi (incidentu ziņošana, politiku izstrāde), pratīsi identificēt galvenos riskus procesos, datu pārvaldībā un darbinieku ikdienā, kā arī veidot drošības kultūru organizācijā. Rezultātā komanda spēs pieņemt pārdomātus, pamatotus lēmumus, cieši sadarbojoties ar IT un drošības speciālistiem un atbildīgajām institūcijām, vienlaikus iegūstot praktisku pamatu budžeta argumentācijai (riski, pasākumi, sagaidāmā ietekme).

Mērķauditorija

Publiskajā pārvaldē nodarbinātie vadītāji (stratēģiskā un operatīvā līmeņa vadītāji).

Programmas moduļi

1. Kiberdrošība kā vadības prioritāte: apdraudējumi, pārvaldība, normatīvie, reputācija un uzticamība.
2. Vadītāja loma kultūrā: “paraugs + komunikācija”, cilvēkfaktors, droša darba vide (paroles, piekļuves, datu aprite).
3. Riska un incidentu vadība: risku identificēšana, kritiskie procesi, rīcības plāns, atbildība un iekšējā/ārējā komunikācija.
4. Ilgtspēja un pārvaldība: politikas/procedūras, mērījumi un uzraudzība, mācības un testi, sadarbība ar HR/IT/juridisko.
5. Pārmaiņu vadība: komunikācija, labās/kļūdu prakses, budžets un resursi, “pietiekami droši”, pēcieviestošanas uzraudzība.
6. Droša digitālo risinājumu ieviešana: ES/LV politika, AI/mākonis u.c., “security/privacy by design”, DPIA un riska lēmumi, datu aprites drošība, IT/juridisko/ārpakalpojumu iesaiste.

Programmas ieguvumi

- Paaugstināta vadītāju spēja identificēt un prioritizēt kiberdrošības riskus, balstot lēmumus datos.
- Vienots incidentu pārvaldības rāmis: skaidras lomas, rīcības soļi un iekšējās/ārējās komunikācijas kārtība.
- Stiprināta kiberdrošības kultūra: konsekventa prasību ievērošana, atbildīga rīcība un darbinieku iesaiste.
- Sakārtota pārvaldība: politikas un procedūras, mērījumi un uzraudzība, regulāras mācības un testi.
- “Security & privacy by design” ieviešana digitālajos projektos, samazinot kļūdu un dārgu pārbūvju risku.
- Labāka sadarbība starp vadību, IT, juristiem un HR, nodrošinot pakalpojumu nepārtrauktību.
- Samazināts incidentu un dīkstāves risks, aizsargāta iestādes reputācija un iedzīvotāju uzticēšanās.
- Praktiski sagatavoti rīki (šabloni, čeklistes, rīcības plāni), ko var ieviest uzreiz pēc mācībām.

ES Atveseļošanas fonda projekts Nr.2.3.2.2.i.0/1/23/I/VARAM/001
"Publiskās pārvaldes digitālā akadēmija"

Digitālā akadēmija

Mācību saturs tiek pielāgots katrai organizācijai/ grupai, ņemot vērā dalībnieku iepriekšējo pieredzi, vajadzības un darba specifiku. Tēmu izklāsts, padziļinājuma līmenis un laika sadalījums katrai tēmai var tikt modificēts atbilstoši konkrētās organizācijas kontekstam/grupai. Tēmas var tikt papildinātas ar citām, kontekstam atbilstošām tēmām un apakštēmām.

Pasniedzēji – nozares vadošie eksperti

Andis Maksimovs
kiberdrošības speciālists ar vairāk nekā desmit gadu pieredzi, Nacionālo bruņoto spēku (NBS) IT drošības jomas profesionālis un pasniedzējs. Viņam ir ilgstoša praktiskā pieredze drošības pārvaldībā NBS sistēmās, kā arī mācībspēka darbs: docējis dažādus ar kiberdrošību saistītus kursus un vadījis seminārus valsts iestādēm (t.sk. CERT.LV platformā). Regulāri uzstājas par kiberdrošības izglītību un sagatavotību un dalās ar praktiskām metodēm, kā veidot noturību un drošības kultūru organizācijās.

Kristaps Felzenbergs
kiberdrošības eksperts, SIA "Routed In" dibinātājs un tehniskais direktors. Vada Vidzemes Augstskolas kiberdrošības inženierzinātņu maģistra programmu un pasniedz ar nozari saistītus kursus. Kristapam ir praktiska pieredze ISO/IEC 27001 standarta ieviešanā un NIS2 prasību īstenošanā, kā arī darbs ar DevOps un mākoņinfrastruktūras arhitektūrām. Ikdienā veido un uztur uzraudzības un žurnāldatu analīzes risinājumus, izmantojot tādus rīkus kā Splunk, Graylog u.c.

Pieteikties

Finansē Eiropas Savienība NextGenerationEU
2027 Nacionālais attīstības plāns
Valsts administrācijas skola
Digitālā akadēmija

ES Atveseļošanas fonda projekts Nr.2.3.2.2.i.0/1/23/I/VARAM/001
"Publiskās pārvaldes digitālā akadēmija"