Aizsardzība pret pikšķerēšanu 4. industriālās revolūcijas laikmetā (CyberPhish)

CyberPhish saīsinātā mācību programma

Projekta ilgums: 2020. gada novembris - 2022. gada novembris

Projekta Nr.: 2020-1-LT01-KA203-078070

Funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

SATURS

IEVADS

Cyberphish saīsinātā mācību programma detalizēti apraksta mācību programmas struktūru, un tās mērķis ir sniegt kodolīgus, bet tālejošus moduļus kiberdrošības jomā, īpašu uzsvaru liekot uz pikšķerēšanas uzbrukumiem. To izmanto ieviešanai augstākās izglītības iestāžu studiju moduļos un izplatīšanas nolūkos, lai piesaistītu dalībniekus kursiem.

Šo īso versiju veido trīs līmeņu tēmas: galvenās tēmas, apakštēmas un apakštēmu punkti, kuru galvenā mērķauditorija ir studenti, citi kursu dalībnieki un pasniedzēji. Tie var izmantot šo mācību programmu, lai izprastu šī kursa galvenos mērķus un uzdevumus.

Svarīgi atzīmēt, ka, lai gan mācību programmas īstenošanā ir paredzēta jaukta mācību pieeja, veids, kā tā ir strukturēta, ļauj elastīgi to īstenot.

Mācību programma nodarbojas ar kiberdrošības ieviešanu, īpašu uzmanību pievēršot pikšķerēšanai. Tā ir paredzēta gan uzņēmumiem, gan privātpersonām kopumā, un tās mērķis ir sagatavot abas puses 4. industriālās revolūcijas laikam un potenciālajām drošības problēmām, ko tā rada.

Mācību programmas ietvaros izglītojamie apgūst prasmes, kā atpazīt un novērst kiberuzbrukumus un kā aizsargāt ierīces un datus pret brutāliem uzbrukumiem.

MĀCĪBU PROGRAMMAS (E-APMĀCĪBAS MODUĻA) STRUKTŪRA

1.1 Ievads

Mācību programma ir paredzēta gan uzņēmumiem, gan indivīdiem, kuri saskarsies ar neizbēgamo pozitīvo un negatīvo ietekmi, ko rada 4. industriālā revolūcija, un kuri vēlas iemācīties un būt vairāk gatavi šīs revolūcijas radīto drošības izaicinājumu pārvarēšanai.

Mācību programmu veido četras atšķirīgas daļas un tā sākas ar ievadu kiberdrošībā un saistītajiem izaicinājumiem, ko rada 4. industriālās revolūcijas iestāšanās. Programmas ietvaros tiek sīkāk aplūkota kiberdrošība un tās juridiskie aspekti Eiropas līmenī, kā arī tas, kā kiberdrošība tiek veicināta Eiropas Savienībā.

Ņemot vērā sociālās inženierijas nozīmi un ietekmi, kā arī tās saistību ar kiberuzbrukumiem, mācību programmā ir izklāstīta kiberuzbrukumu atpazīšana un atbilstoša rīcība, lai izvairītos no postošām un neatgriezeniskām sekām.

Papildus īsam dažādu moduļu aprakstam, mācību programmas struktūra ietver katra moduļa mācību mērķus un ieteicamo ilgumu un mācīšanas modalitātes. Ir svarīgi atzīmē, ka lai gan mācību programmā norādīts noteikts stundu skaits katrā modulī, šīs stundas jāuzskata par kontaktstundām. Pilna mācību programma kopā prasa 30 stundas, kas atbilst 1 ECTS. Tiek rekomendēts paredzēt tādu pašu stundu skaitu katrā modulī pašmācībai un novērtēšanai.

Mācību programmas modulis	***Moduļa mērķis***
1.0 Ievads kiberdrošībā	Šī moduļa mērķis ir iepazīstināt gan trenerus, gan studentus ar kiberdrošības kursu un tā tēmām. Tas sākas ar īsu kibernoziedzības attīstības vēsturi un tās straujās izaugsmes iemesliem, kā arī vēsturiskajiem posmiem un pašreizējo situāciju. Tajā izklāstīti arī kiberuzbrukuma radītie izaicinājumi, ar ko saskaras indivīdi un uzņēmumi līdz ar 4. industriālās revolūcijas atnākšanu, tostarp, bet ne tikai globālo robežu mazināšanos, izplatītu mobilo tehnoloģiju lietošanu, mākoņdatošanu, lietu

		internetu un lielajiem datiem. Citi izaicinājumi ir saistīti ar trešo pušu riskiem un pieaugošajiem draudiem, tostarp valstu drošības apdraudējumiem. Treneri varēs atrast nepieciešamo materiālu, lai iepazīstinātu izglītojamos ar kiberdrošības koncepciju, kā arī izaicinājumiem, ar kuriem parasti saskaras uzņēmumi, kur tas iespējams, aplūkojot reālus scenārijus. Modulī sīkāk aplūkotas vairākas definīcijas un žargons, kas tiek izmantots kiberdrošības nozarē.
2.0	Pārskats par kiberdrošību ES	Šis modulis iepazīstina izglītojamo ar pašreizējām ES politikām un iniciatīvām, kuru mērķis ir veicināt kiberdrošības jēdzienu. Tajā aplūkoti arī kiberdrošības juridiskie aspekti gan ES, gan visā pasaulē, ļaujot izglītojamajiem iepazīties ar daudziem reālās dzīves scenārijiem un gadījumu izpēti šajā jomā. Modulis ietver pārskatu par kiberdrošības tendencēm, tostarp, bet ne tikai statistiku, attīstības tendencēm, būtiskajiem apdraudējumiem, juridiskajiem, reputācijas un finanšu riskiem un gadījumu izpētes analīzi.
3.0	Kiberuzbrukumi - sociālā inženierija un pikšķerēšana	Šis modulis iepazīstina izglītojamo ar kiberuzbrukumiem, īpašu uzmanību pievēršot pikšķerēšanai. Tajā arī detalizēti aplūkoti sociālās inženierijas un reversās sociālās inženierijas jēdzieni, kā arī sociālās inženierijas ciešā saikne ar kiberuzbrukumiem. Moduļa ietvaros tiek aplūkoti arī dažādi pikšķerēšanas uzbrukumu veidi un paņēmieni, kā arī vairāki reāli gadījumu izpētes piemēri no projekta partnervalstīm.
4.0	Kiberuzbrukumu izpratne un rīcība kiberuzbrukuma gadījumā	Šis modulis iepazīstina izglītojamo ar e-drošības jēdzienu un par proaktīvas pieejas kiberdraudiem nozīmi, izmantojot kiberhigiēnas koncepciju. Modulī arī sīkāk aplūkota pieeja kiberuzbrukumu atpazīšanai un novēršanai. Modulis iepazīstina ar incidentu reaģēšanas plānu izstrādi un ieviešanu, lai mazinātu kiberuzbrukumu sekas.

1.2 Detalizēta e-apmācības moduļa struktūra

1.2.1 Ievads kiberdrošībā

Moduļa nosaukums	1.0 Ievads kiberdrošībā
Kopējais ilgums *(Stundas / slaidi)*	3 stundas 46 - 60 slaidi
Pasniegšanas metodes	Klātienē Tiešsaistē Jaukta pasniegšanas metode
Novērtējums	Klātienes / tiešsaistes tests

<table>
<tr><td>Mācību rezultāti</td><td>

Vispārēja izpratne par kiberdrošību
Izpratne par kiberdrošības izaicinājumiem
Izpratne par to, kā kiberuzbrukumi ir mainījušies laika gaitā, kā rezultātā pastiprinājušies kiberuzbrukumu darbības un tādējādi arī pretpasākumi
Izpratne par to, kādēļ ir svarīgi sekot līdzi kiberdrošības jaunumiem un kādēļ ir nepieciešams pastāvīgi atjaunināt zināšanas par kiberdrošību
Izpratne par dažādām ar kiberdrošību saistītām definīcijām

</td></tr>
<tr><td>Prasības</td><td>Sākotnējās zināšanas nav nepieciešamas</td></tr>
<tr><td>Moduļa apraksts</td><td>
Šī moduļa mērķis ir iepazīstināt gan trenerus, gan studentus ar kiberdrošības kursu un tā tēmām. Tas sākas ar īsu kibernoziedzības attīstības vēsturi un tās straujās izaugsmes iemesliem, kā arī vēsturiskajiem posmiem un pašreizējo situāciju.

Tajā izklāstīti arī kiberuzbrukuma radītie izaicinājumi, ar ko saskaras indivīdi un uzņēmumi līdz ar 4. industriālās revolūcijas atnākšanu, tostarp, bet ne tikai globālo robežu mazināšanos, izplatītu mobilo tehnoloģiju lietošanu, mākoņdatošanu, lietu internetu un lielajiem datiem. Citi izaicinājumi ir saistīti ar trešo pušu riskiem un pieaugošajiem draudiem, tostarp valstu drošības apdraudējumiem.

Treneri varēs atrast nepieciešamo materiālu, lai iepazīstinātu izglītojamos ar kiberdrošības koncepciju, kā arī izaicinājumiem, ar kuriem parasti saskaras uzņēmumi, kur tas iespējams, aplūkojot reālus scenārijus.

Modulī sīkāk aplūkotas vairākas definīcijas un žargons, kas tiek izmantots kiberdrošības nozarē.
</td></tr>
<tr><td colspan="2">MODUĻA APAKŠTĒMAS</td></tr>
<tr><td>1.1 Vispārīga informācija - 4. industriālās revolūcijas izaicinājumi</td><td>

Ievads kiberdrošībā
Īsa kibernoziedzības attīstības vēsture un tās straujās izaugsmes iemesli, kā arī vēsturiskie posmi un pašreizējā situācija
Vispārīga informācija par problēmu, iezīmējot kiberuzbrukumu radītos izaicinājumus, ar ko saskaras uzņēmumi
Izaicinājumi, ar ko saskaras uzņēmumi:

Nav robežu;
Tehnoloģijas: Plaša tehnoloģiju (mobilo tehnoloģiju) izmantošana;
Mākoņdatošana;
Lielo datu izaicinājumi;
Trešo personu riski;
Lietu internets;

Pieaugošo draudu izaicinājums;
Valstu apdraudējumi

<table>
<tr><td>Ieteicamais ilgums stundās

1,5</td><td>Minimālais slaidu skaits

23</td><td>Maksimālais slaidu skaits

30</td></tr>
</table>
</td></tr>
</table>

1.2	**Kiberdrošības vēsture**	• Īss izklāsts par to, kā kiberuzbrukumi ir mainījušies laika gaitā, kā rezultātā pastiprinājušies kiberuzbrukumu darbības un tādējādi arī pretpasākumi. • Šajā sadaļā var tikt iekļauti vietējie / Eiropas / starptautiskie gadījumu pētījumi	
		Ieteicamais ilgums stundās 1,0	*Minimālais slaidu skaits* 15	*Maksimālais slaidu skaits* 20
1.3	**Kiberdrošības definīcijas**	• Sadaļa par kiberdrošības žargonu / terminiem un statistiku / avotiem	
		Ieteicamais ilgums stundās 0,5	*Minimālais slaidu skaits* 8	*Maksimālais slaidu skaits* 10

1.2.2 Kiberdrošība Eiropas Savienībā (ES)

Moduļa nosaukums	2.0 Kiberdrošība ES
Kopējais ilgums *(Stundas / slaidi)*	3 stundas 48 - 67 slaidi
Pasniegšanas metode	Klātienē Tiešsaistē Jaukta pasniegšanas metode Diskusijas
Novērtējums	Klātienes / tiešsaistes tests
Mācību rezultāti	• Kiberdrošības juridisko aspektu izpratne • Izpratne par pašreizējo ES politiku saistībā ar kiberdrošību • Izpratne par ES tiesību aktiem, kas saistīti ar kiberdrošību • Kiberdrošības vietējo likumu saistīšana un salīdzināšana ar ES tiesību aktiem
Prasības	IT un biznesa pamatzināšanas varētu būt noderīgas, lai labāk izprastu moduli
Moduļa apraksts	Šis modulis iepazīstina izglītojamo ar pašreizējām ES politikām un iniciatīvām, kuru mērķis ir veicināt kiberdrošības jēdzienu. Tajā aplūkoti arī kiberdrošības juridiskie aspekti gan ES, gan visā pasaulē, ļaujot izglītojamajiem iepazīties ar daudziem reālās dzīves scenārijiem un gadījumu izpēti šajā jomā. Modulis ietver pārskatu par kiberdrošības tendencēm, tostarp, bet ne tikai statistiku, attīstības tendencēm, būtiskajiem apdraudējumiem, juridiskajiem, reputācijas un finanšu riskiem un gadījumu izpētes analīzi.
MODUĻA APAKŠTĒMAS	

2.1	**Kiberdrošības veicināšana Eiropas Savienībā**	• Īss ievads par ES politiku un iniciatīvām, kuru mērķis ir veicināt kiberdrošības jēdzienu		
		Ieteicamais ilgums stundās 1,0	*Minimālais slaidu skaits* 20	*Maksimālais slaidu skaits* 30
2.2	**Kiberdrošības juridiskie aspekti**	• Kiberdrošības juridiskie aspekti visā pasaulē (vispārīgi) un jo īpaši ES, tostarp neatbilstības sekas • Kiberdrošības vietējo likumu saistība, salīdzinājums un kontrasts ar ES likumiem		
		Ieteicamais ilgums stundās 0,5	*Minimālais slaidu skaits* 5	*Maksimālais slaidu skaits* 7
2.3	**Pārskats par kiberdrošības tendencēm**	• Reālo dzīves scenāriju un gadījumu izpēte, ieskaitot statistiku, tendences, attiecīgos draudus, riskus (juridiskos, reputācijas, finanšu) • Ieskats nesenajos kiberuzbrukumos un diskusijas par kvalifikācijas celšanas nozīmi, ņemot vērā iespējamos kiberuzbrukumu riskus. *Piezīme: Diskusija var noritēt tiešsaistē vai klātienē. Treneris vada diskusiju un sniedz norādes par to, kas sagaidāms no diskusijas.*		
		Ieteicamais ilgums stundās 1,5	*Minimālais slaidu skaits* 23	*Maksimālais slaidu skaits* 30

1.2.3 Kiberuzbrukumi: Sociālā inženierija un pikšķerēšana

Moduļa nosaukums	3.0 Kiberuzbrukumi: Sociālā inženierija un pikšķerēšana
Kopējais ilgums *(Stundas / slaidi)*	10 stundas 150 - 200 slaidi
Pasniegšanas metode	Klātienē Tiešsaistē Jaukta pasniegšanas metode Interaktīvu rīku (piemēram, tiešsaistes scenāriju rīku) izmantošana Diskusijas
Novērtējums	Klātienes / tiešsaistes tests
Mācību rezultāti	• Izprot kiberuzbrukumu jēdzienu • Spēj definēt sociālo inženieriju un apgriezto sociālo inženieriju • Izprot sociālās inženierijas modalitāti un tās saistību ar kiberuzbrukumiem • Izprot visbiežāk sastopamos kiberdrošības draudus • Izprot galvenās kiberuzbrukumu kategorijas un paņēmienus

<table>
<tr><td>Prasības</td><td colspan="3">IT un biznesa pamatzināšanas varētu būt noderīgas, lai labāk izprastu moduli</td></tr>
<tr><td>Moduļa apraksts</td><td colspan="3">Šis modulis iepazīstina izglītojamo ar kiberuzbrukumiem, īpašu uzmanību pievēršot pikšķerēšanai. Tajā arī detalizēti aplūkoti sociālās inženierijas un reversās sociālās inženierijas jēdzieni, kā arī sociālās inženierijas ciešā saikne ar kiberuzbrukumiem.

Moduļa ietvaros tiek aplūkoti arī dažādi pikšķerēšanas uzbrukumu veidi un paņēmieni, kā arī vairāki reāli gadījumu izpētes piemēri no projekta partnervalstīm.</td></tr>
<tr><td colspan="4">MODUĻA APAKŠTĒMAS</td></tr>
<tr><td rowspan="2">3.1 Ievadinformācija par kiberuzbrukumiem</td><td colspan="3">• Īsa ievadinformācija par kiberuzbrukumiem, jo īpaši pikšķerēšanas uzbrukumiem</td></tr>
<tr><td>Ieteicamais ilgums stundās

0,5</td><td>Minimālais slaidu skaits

8</td><td>Maksimālais slaidu skaits

10</td></tr>
<tr><td rowspan="2">3.2 Sociālās inženierijas moduļi un manipulācijas</td><td colspan="3">• Sociālo inženierijas modeļu pārskats, īpašu uzmanību pievēršot šādiem aspektiem:

a) “Ietekmes ieroči” - R. Cialdini[1]
- Atbildes darbība
- Apņemšanās un konsekvence
- Sociālie pierādījumi
- Patika
- Autoritāte
- Trūkums

b) Sociālās inženierijas psiholoģiskie aspekti
c) Pārskats par reverso sociālo inženieriju</td></tr>
<tr><td>Ieteicamais ilgums stundās

4</td><td>Minimālais slaidu skaits

60</td><td>Maksimālais slaidu skaits

80</td></tr>
<tr><td>3.3 Dažādi pikšķerēšanas uzbrukumu veidi un paņēmieni</td><td colspan="3">• Šajā sadaļā tiek definēti dažādi kiberuzbrukumu veidi (jo īpaši, pikšķerēšana) un tas, kā tos atpazīt (nākamā nodaļa), tostarp, bet ne tikai:

Kategorijas
- Ar VDAR saistīti uzbrukumi
- E-pasti;
- Tūlītējā ziņojumapmaiņa;
- Sociālie tīkli;
- Tīmekļa vietnes;
- Izkrāpšana ar loterijas palīdzību;
- SMS;</td></tr>
</table>

[1] Cialdini, R. B. (2016). Pre-Suasion: A Revolutionary Way to Influence and Persuade. New York: Simon & Schuster. ISBN 978-1501109799.

	- Tālruņa zvani; - Klātienē; - "Sērfošana uz citu pleciem"; **Dažādu tehniku apvienojums** - "Spray and Pray" jeb masveida pikšķerēšana - "Spear phishing" jeb mērķtiecīga pikšķerēšana - "Whaling" jeb vaļu medības - "Vishing" jeb balss pikšķerēšana - "Smishing" jeb SMS pikšķerēšana - "Angler Phishing" jeb klientu apkalpošanas pikšķerēšana - "Clone phishing" jeb klona pikšķerēšana - "Malvertising" jeb ļaunprātīgas reklāmas		
	Ieteicamais ilgums stundās 4	*Minimālais slaidu skaits* 60	*Maksimālais slaidu skaits* 80
3.4 Gadījumu izpēte	• Vairāku dažādu partnerorganizāciju veiktu gadījumu pētījumu prezentācija • Tiešsaistes vai klātienes diskusija mazās grupās (5-6 studenti) *Piezīme: Diskusija notiek kā vingrinājums, katrai grupai atrodot un analizējot nesenu pikšķerēšanas uzbrukumu, iekļaujot tādu informāciju kā uzbrukuma datums, informācija par upuri, uzbrukuma modalitāte, sekas, gūtās mācības un tā tālāk. Pēc tam izglītojamais no katras grupas iepazīstina pārējos ar analīzes rezultātiem. Treneris un kolēģi sniedz konstruktīvas atsauksmes.*		
	Ieteicamais ilgums stundās 1,5	*Minimālais slaidu skaits* 22	*Maksimālais slaidu skaits* 30

1.2.4 Kiberuzbrukumu izpratne un rīcība kiberuzbrukuma gadījumā

Moduļa nosaukums	4.0 Kiberuzbrukumu izpratne un rīcība kiberuzbrukuma gadījumā
Kopējais ilgums *(Stundas / slaidi)*	14 stundas 210 - 255 slaidi
Pasniegšanas metode	Klātienē Tiešsaistē Jaukta pasniegšanas metode
Novērtējums	Klātienes / tiešsaistes tests
Mācību rezultāti	• Apgūt pamatzināšanas par e-drošību un drošību • Izprot dažādu informācijas saturu • Izprot identitāti un nošķirt dažādus uzbrukumus, kas saistīti ar identitāti • Izprot kiberuzbrukumu radītās sekas indivīdiem un/vai organizācijām

<table>
<tr><td></td><td colspan="3">• Definē un izprot kiberhigiēnas kā proaktīvas darbības pret kiberuzbrukumiem nozīmi
• Izprot un izmanto dažādas aizsardzības metodes pret kiberuzbrukumiem
• Izstrādā un ievieš rīcības plānu reaģēšanai uz kiberuzbrukumu</td></tr>
<tr><td>Prasības</td><td colspan="3">Iepriekšējie moduļi</td></tr>
<tr><td>Moduļa apraksts</td><td colspan="3">Šis modulis iepazīstina izglītojamo ar e-drošības jēdzienu un par proaktīvas pieejas kiberdraudiem nozīmi, izmantojot kiberhigiēnas koncepciju.

Modulī arī sīkāk aplūkota pieeja kiberuzbrukumu atpazīšanai un novēršanai.

Modulis iepazīstina ar incidentu reaģēšanas plānu izstrādi un ieviešanu, lai mazinātu kiberuzbrukumu sekas.</td></tr>
<tr><td colspan="4">MODUĻA APAKŠTĒMAS</td></tr>
<tr><td>4.1 Pamatzināšanas par e-drošību</td><td colspan="3">• Informācijas satura atšķirības (atklāta, privāta, biznesa u.t.t.); Intelektuālais īpašums; Autortiesības;
• Izpratne par identitātes terminu; zināšanas par identitātes zādzībām un zādzības metodēm. Informācija par spiegprogrammatūru, tastatūras spiegiem, krāpniecisku reklāmu, Trojas zirgiem. Zina dažādus veidus, kā ļaunprātīga programmatūra var iekļūt ierīcē.
• Zina par identitātes un personas datu zādzību cēloņiem un sekām darbavietā un internetā (krāpnieciska informācijas izmantošana, informācijas zuduma draudi, sabotāža).
• Zina par draudiem, kas saistīti ar personas datu izpaušanu.
• Īss ievads par kiberuzbrukumu sekām gan indivīdam, gan organizācijai. Papildu informācija jāizpēta 4.4. sadaļā.</td></tr>
<tr><td></td><td>Ieteicamais ilgums stundās
0,5</td><td>Minimālais slaidu skaits
8</td><td>Maksimālais slaidu skaits
10</td></tr>
<tr><td>4.2 Proaktīvas darbības</td><td colspan="3">• Kiberhigiēna internetā (līdz minimumam samaziniet informāciju par personām, tostarp informāciju personīgajos kontos sociālajos medijos, ko uzbrucēji varētu izmantot)
• Kiberhigiēna darba vietā
• Tehnoloģiskie rīki un pasākumi (pikšķerēšanas e-pastu filtrēšana un bloķēšana)</td></tr>
<tr><td></td><td>Ieteicamais ilgums stundās
2</td><td>Minimālais slaidu skaits
30</td><td>Maksimālais slaidu skaits
35</td></tr>
</table>

<table>
<tr><td>4.3.</td><td>Pikšķerēšanas uzbrukumu atpazīšana</td><td colspan="3">

Gadījumu izpētes analīze, izmantojot 3.3. sadaļā - Dažādi pikšķerēšanas uzbrukumu veidi un paņēmieni minētos paņēmienus
Sadaļa kiberuzbrukumu atpazīšanai (atsaucoties uz iepriekšējās nodaļas punktiem), tostarp, bet ne tikai:

Kritiskā domāšana
Saišu pārbaude
Izpratne par URL
Ziņojumu analīze
Sarkano karogu atpazīšana

<table>
<tr><td>Ieteicamais ilgums stundās
5</td><td>Minimālais slaidu skaits
75</td><td>Maksimālais slaidu skaits
90</td></tr>
</table>
</td></tr>
<tr><td>4.4</td><td>Rīcība kiberuzbrukumu gadījumā</td><td colspan="3">

Informācija par kiberdrošību, tostarp informācija par kaitējumu, ko kiberuzbrukumi nodada indivīdiem un organizācijām, un to, kā rīkoties kiberuzbrukuma gadījumā, balstoties uz iepriekšējā nodaļā apgūto.
Cita starpā, jāiekļauj šādi aspekti:

Droša navigācija
Spēcīgu paroļu izveide
Izvairīšanās no uzbrukumiem
Droša iepirkšanās tiešsaistē
Pretkiberuzbrukumu programmatūras instalēšana
Sīkdatnes
Atbilstošu dublējumu izveide
Failu šifrēšana
Divu faktoru autentifikācija
Ļaunprogrammatūra
Droša pārlūkošana

Šajā sadaļā tiek iekļauti arī vietējie / Eiropas / starptautiskie gadījumu pētījumu piemēri, kas minēti iepriekšējos moduļos.
Kur tas nepieciešams, šajā sadaļā ietver vienkāršas soli pa solim instrukcijas un attālus.
Šajā sadaļā iekļauta informācija par darbībām, kas jāveic, reaģējot uz kiberuzbrukumu, tostarp atkopšanas procedūras, ja organizācija un/vai lietotājs kļūst par kiberuzbrukuma upuriem.

<table>
<tr><td>Ieteicamais ilgums stundās
5</td><td>Minimālais slaidu skaits
75</td><td>Maksimālais slaidu skaits
90</td></tr>
</table>
</td></tr>
<tr><td>4.5</td><td>Kaitējuma mazināšana, reaģējot uz incidentiem</td><td colspan="3">

Incidentu reaģēšanas plānu izstrāde, attīstīšana un īstenošana, norādot rekomendētās darbības un labāko praksi, ko nepieciešams īstenot datu aizsardzības pārkāpuma gadījumā.
Piezīme: Šīs sadaļas elementus var pielāgot konkrēto valstu vajadzībām.

<table>
<tr><td>Ieteicamais ilgums stundās
1,5</td><td>Minimālais slaidu skaits
22</td><td>Maksimālais slaidu skaits
30</td></tr>
</table>
</td></tr>
</table>