Prevencinės priemonės kovai su fišingu 4-osios pramonės revoliucijos amžiuje (CyberPhish)

„CyberPhish“ mokymo programos santrumpa

Projekto trukmė: 2020 lapkritis – 2022 lapkritis

Project 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.

Turinys

ĮVADAS

„Cyberphish“ mokymo programos santrumpoje pateikiama detali kurso struktūra bei dėstomi dalykai (moduliai), kuriais siekiama ugdyti studentų žinias, susijusias su kibernetiniu saugumu, o ypač sukčiavimo (angl. phishing) atakomis (duomenų vagystėmis). Projekto metu sukaupta patirtis bus naudojama dėstant modulius aukštosiose mokyklose ir siekiant šia programa sudominti įvairius asmenis.

Trumpąją programos versiją sudaro trys dalys: pagrindinis dalykas, temos ir jose pateikiamos užduotys. Kursas sieks ugdyti ne tik studentus, bet ir kitus dalyvius bei dėstytojus. Jie gali naudotis šiuo planu, siekdami geriau suprasti pagrindinius programos tikslus ir siekinius.

Svarbu pažymėti, jog nors planuojama dėstyti programą mišriu būdu, jos struktūra sudaryta taip, jog šią įmanoma pritaikyti priklausomai nuo tuo metu susidariusios situacijos.

Viso kurso esmė – supažindinti su kibernetine sauga, didelį dėmesį skiriant sukčiavimo (angl. phishing) atakoms. Jis skirtas individualiems asmenims, verslininkams ir sieks parengti Pramonei 4.0 bei kartu su ja kylančiomis saugumo grėsmėmis.

Mokymo programos metu, besimokantieji įgaus įgūdžių, susijusių su kibernetinių atakų atpažinimu bei, kaip nuo jų apsaugoti savo įrenginius ar duomenis.

1. MOKYMO PROGRAMOS (NUOTOLINIU BŪDU) STRUKTŪRA

1.1 Programos pagrindinės temos

Mokymo programos tikslas – suteikti daugiau žinių tiek individualiems asmenims, tiek verslininkams, kurie patiria neišvengiamas teigiamas ir neigiamas Pramonės 4.0 pasekmes ir nori pagerinti savo įgūdžius, susijusius su kibernetine sauga.

Mokymo programa sudaryta iš keturių atskirų dalių, pradedant įvadu į kibernetinio saugumo sritį ir su ja susijusius iššūkius, kylančius dėl Pramonės 4.0. Joje gilinamasi į kibernetinį saugumą ir jo teisinius aspektus Europos lygmeniu, taip pat į tai, kaip kibernetinis saugumas skatinamas Europos Sąjungoje.

Atsižvelgiant į socialinės inžinerijos svarbą ir poveikį bei jos ryšį su kibernetinėmis atakomis, šiame kurse aiškinama, kaip atpažinti kibernetines atakas ir kaip su jomis elgtis, kad būtų išvengta didelių ir negrįžtamų padarinių.

Kartu su glaustu įvairių modulių aprašymu, mokymo programoje pateikiami kiekvieno modulio mokymosi rezultatai, siūlomos rekomenduojamos valandos ir mokymosi būdai. Reikėtų pažymėti, kad nors mokymo programoje nurodytas valandų skaičius kiekvienam moduliui, šios valandos laikytinos kontaktinėmis valandomis. Visą mokymo programą sudaro 30 valandų, kurios atitinka 1 ECTS. Rekomenduojama, kad toks pat valandų skaičius kiekvienam moduliui būtų skirtas savarankiškam mokymuisi ir vertinimui.

Dalykas (modulis)	*Dalyko (modulio) tikslas*
1.0 Kibernetinio saugumo įvadas	Supažindinti su kibernetiniu saugumu bei įvairiomis temomis tiek dėstytojus, tiek studentus, besimokančius aukštosiose mokyklose. Pradedama nuo trumpos kibernetinių nusikaltimų tobulėjimo istorijos ir priežasčių, kurios lėmė spartų jų masto augimą, įvairių istorinių etapų bei dabartinės situacijos apibūdinimo. Apibūdinami dėl 4.0 Pramonės kylantys sunkumai, su kuriais susiduria tiek individualūs asmenys, tiek verslininkai. Vieni iš jų yra globalizacija, augantis mobiliųjų technologijų poreikis, debesijos platformos, daiktų internetas ir didieji duomenys. Be to galima paminėti trečiųjų šalių ir nacionalinio masto grėsmes. Dėstytojai galės rasti reikiamos medžiagos, kad supažindintų besimokančiuosius su kibernetinio saugumo sąvoka kartu su įprastais iššūkiais, su kuriais susiduria įmonės, jei įmanoma, pasitelkdami realių atvejų scenarijus. Taip pat bus nagrinėjamos įvairios sąvokos bei žargonai, kurie susiję su kibernetiniu saugumu.
2.0 Kibernetinė sauga Europos Sąjungoje (ES)	Šis modulis supažindina su esama ES politika ir iniciatyvomis, kuriomis siekiama skatinti kibernetinio saugumo koncepciją. Jame taip pat aptariami teisiniai kibernetinio saugumo aspektai tiek ES, tiek visame pasaulyje, supažindinama su daugybe realių šios srities scenarijų ir atvejų analizių. Modulyje apžvelgiamos Kibernetinio saugumo srities tendencijos, įskaitant, bet neapsiribojant statistiniais duomenimis, tendencijomis, atitinkamomis grėsmėmis, teisine, reputacijos ir finansine rizika bei atvejų analize.
3.0 Kibernetinės atakos (socialinė inžinerija ir sukčiavimas (angl. phishing)	Šiame modulyje mokiniai supažindinami su kibernetinėmis atakomis, ypatingą dėmesį skiriant sukčiavimo (angl. phishing) atakoms. Modulyje taip pat išsamiai aptariama socialinės inžinerijos ir atvirkštinės socialinės inžinerijos sąvoka bei aiškinamasi, kaip socialinė inžinerija susijusi su kibernetinėmis atakomis. Modulyje taip pat pristatomos įvairių tipų sukčiavimo (angl. phishing) atakos ir metodai, taip pat pateikiami keli realūs pavyzdžiai iš projekto partnerių šalių.
4.0 Kibernetinių atakų atpažinimas ir apsauga	Šiame modulyje studentai supažindinami su e. saugos sąvoka ir aktyvaus požiūrio į kibernetines grėsmes svarbą, taikant kibernetinės higienos koncepciją. Modulyje taip pat išsamiai aprašoma, kaip atpažinti kibernetines atakas ir kaip su jomis elgtis. Modulis supažindina su reagavimo į incidentus planų kūrimu ir įgyvendinimu, siekiant sumažinti kibernetinių atakų poveikį.

1.2 Detali mokymo nuotoliniu būdu programos struktūra

1.2.1 Kibernetinio saugumo įvadas

Dalyko (modulio) pavadinimas	1.0 Kibernetinio saugumo įvadas
Bendra trukmė *(valandomis / skaidrėmis)*	3 valandos 46–60 skaidrių
Mokymo metodai	Kontaktiniu būdu, Nuotoliniu būdu, Mišriuoju būdu.
Vertinimas	Kontaktiniu būdu ar internetiniu testu.
Dalyko (modulio) siekiniai	• Turėti bendrų kibernetinio saugumo žinių. • Suprasti kibernetinio saugumo keliamus iššūkius. • Suprasti, kaip laikui bėgant keitėsi kibernetinės atakos, dėl kurių atsirado daugiau priemonių, taigi ir kovos su kibernetinėmis atakomis priemonių. • Suprasti, kodėl svarbu sekti kibernetinio saugumo situaciją, ir kodėl būtina nuolat atnaujinti kibernetinio saugumo žinias. • Suprasti įvairias su kibernetiniu saugumu susijusias apibrėžtis.
Išankstiniai reikalavimai	Nėra
Dalyko (modulio) aprašas	Šio modulio tikslas – supažindinti aukštųjų mokyklų dėstytojus ir studentus su kibernetinio saugumo kursu ir jo temomis. Jis pradedamas trumpa kibernetinio saugumo raidos istorija ir jo spartaus augimo priežastimis, taip pat istoriniais etapais ir dabartine padėtimi. Taip pat apibūdinami kibernetinių atakų iššūkiai, su kuriais susiduria asmenys ir įmonės Pramonės 4.0 amžiuje, įskaitant, bet neapsiribojant, sumažėjusias pasaulines ribas, plačiai naudojamas mobiliąsias technologijas, debesų kompiuteriją, daiktų internetą (IoT) ir didžiuosius duomenis. Kiti iššūkiai apima trečiųjų šalių riziką ir didėjančias grėsmes, įskaitant nacionalinių valstybių (angl. nations-states) grėsmes. Dėstytojai galės rasti reikiamos medžiagos, kad supažindintų besimokančiuosius su kibernetinio saugumo sąvoka kartu su įprastais iššūkiais, su kuriais susiduria įmonės, jei įmanoma, pasitelkdami realių atvejų scenarijus. Modulyje taip pat gilinamasi į daugybę Kibernetinio saugumo srityje vartojamų ir sutinkamų apibrėžčių ir žargono.

<table>
<tr><th colspan="4">DALYKO (MODULIO) TEMOS</th></tr>
<tr><td>1.1 Įvadas: ketvirtosios pramonės revoliucijos iššūkiai</td><td colspan="3">• Kibernetinio saugumo įvadas.
• Trumpa kibernetinių nusikaltimų istorija bei priežastys, kurios lėmė spartų jų masto augimą bei dabartinė situacija.
• Problemos su kuriomis susiduria verslas, prieš kurį nukreipiamos kibernetinės atakos.
• Verslui kylantys iššūkiai:
- išnykusios ribos,
- technologijos ir platus jų naudojimas (mobiliosios technologijos),
- debesų kompiuterija,
- sunkumai, susiję su didžiaisiais duomenimis,
- trečiųjų šalių grėsmė,
- daiktų internetas.
• Didėjančių grėsmių iššūkiai.
• Valstybinio mąsto grėsmės.</td></tr>
<tr><td></td><td>Rekomenduojama trukmė
1 val. 30 min.</td><td>Mažiausiai skaidrių
23</td><td>Daugiausiai skaidrių
30</td></tr>
<tr><td>1.2 Kibernetinio saugumo istorija</td><td colspan="3">• Trumpa kibernetinio saugumo istorija, dėl kurios laikui bėgant, keitėsi požiūris į tokio pobūdžio atakas, bei kokie metodai taikomi, siekiant apsisaugoti nuo atakų.
• Lokalių, Europos, tarptautinių atvejų analizė.</td></tr>
<tr><td></td><td>Rekomenduojama trukmė
1 valanda</td><td>Mažiausiai skaidrių
15</td><td>Daugiausiai skaidrių
20</td></tr>
<tr><td>1.3 Kibernetinio saugumo apibrėžimai</td><td colspan="3">• Šioje dalyje nagrinėjami kibernetinio saugumo apibrėžimai ir žargonai bei statistika ir šaltiniai.</td></tr>
<tr><td></td><td>Rekomenduojama trukmė
30 min.</td><td>Mažiausiai skaidrių
8</td><td>Daugiausiai skaidrių
10</td></tr>
</table>

1.2.2 Kibernetinė sauga Europos Sąjungoje (ES)

Dalyko (modulio) pavadinimas	2.0 Kibernetinė sauga Europos Sąjungoje (ES)
Bendra trukmė *(valandomis / skaidrėmis)*	3 valandos 48–67 skaidrės
Mokymo metodai	Kontaktiniu būdu, Nuotoliniu būdu, Mišriuoju būdu, Diskusijomis.
Vertinimas	Kontaktiniu būdu ar internetiniu testu.
Dalyko (modulio) siekiniai	• Suprasti kibernetinio saugumo teisinius aspektus. • Suprasti dabartinės ES politikos kibernetinio saugumo klausimus. • Suprasti ES įstatymus, susijusius su kibernetine sauga. • Susieti ir palyginti kibernetinio saugumo vietos teisės aktus ir ES teisės aktus.
Išankstiniai reikalavimai	Pagrindinės IT ir verslo žinios gali būti naudingos norint geriau suprasti modulį
Dalyko (modulio) aprašymas	Šis modulis supažindina su esama ES politika ir iniciatyvomis, kuriomis siekiama skatinti kibernetinio saugumo koncepciją. Jame taip pat aptariami teisiniai kibernetinio saugumo aspektai tiek ES, tiek visame pasaulyje, supažindinama su daugybe realių šios srities scenarijų ir atvejų analizių. Modulyje apžvelgiamos Kibernetinio saugumo srities tendencijos, įskaitant, bet neapsiribojant statistiniais duomenimis, tendencijomis, atitinkamomis grėsmėmis, teisine, reputacijos ir finansine rizika bei atvejų analize.

<table>
<tr><th colspan="4">DALYKO (MODULIO) TEMOS</th></tr>
<tr><td rowspan="2">2.1 Kibernetinio saugumo ugdymas Europos Sąjungoje</td><td colspan="3">• Trumpas supažindinimas su ES strategijomis bei iniciatyvomis, kuriomis siekiama šviesti asmenis kibernetinio saugumo klausimais.</td></tr>
<tr><td>Rekomenduojama trukmė
1 valanda</td><td>Mažiausiai skaidrių
20</td><td>Daugiausiai skaidrių
30</td></tr>
<tr><td rowspan="2">2.2 Kibernetinio saugumo teisiniai aspektai</td><td colspan="3">• ES teisiniai aspektai bei atsakomybė, kuri gresia už jų nesilaikymą bei bendrinis tarptautinių teisinių aspektų aptarimas.
• ES ir tarptautinių kibernetinio saugumo įstatymų santykis, palyginimas ir skirtumai.</td></tr>
<tr><td>Rekomenduojama trukmė
30 min.</td><td>Mažiausiai skaidrių
5</td><td>Daugiausiai skaidrių
7</td></tr>
<tr><td rowspan="2">2.3 Kibernetinio saugumo tendencijų apžvalga</td><td colspan="3">• Realių pavyzdžių pristatymas bei atvejų analizė kartu su statistika, tendencijomis, potencialiomis grėsmėmis ir galima žala (teisine, įvaizdžio ar finansine prasme).
• Žvilgsnis į pastaruoju metu įvykdytas kibernetines atakas bei diskusija auditorijoje apie kompetencijos svarbą, kurią dėl kibernetinių atakų, asmenys privalo nuolatos gerinti.
Pastaba: diskusija gali vykti tiek kontaktiniu, tiek nuotoliniu būdu padedant dėstytojui, kuris nustato diskusijos tvarką ir pabrėžia, ko iš jos galima tikėtis.</td></tr>
<tr><td>Rekomenduojama trukmė
1 val. 30 min.</td><td>Mažiausiai skaidrių
23</td><td>Daugiausiai skaidrių
30</td></tr>
</table>

1.2.3 Kibernetinės atakos (socialinė inžinerija ir sukčiavimas (angl. phishing))

Dalyko (modulio) pavadinimas	3.0 Kibernetinės atakos (socialinė inžinerija ir sukčiavimas (angl. phishing))
Bendra trukmė *(valandomis / skaidrėmis)*	10 valandų 150–200 skaidrių
Mokymo metodai	Kontaktiniu būdu, Nuotoliniu būdu, Mišriuoju būdu, Interaktyvių įrankių naudojimas (pvz. internetinių situacijų įrankių), Diskusijos.
Vertinimas	Kontaktiniu būdu ar internetiniu testu.
Dalyko (modulio) siekiniai	• Suprasti kibernetinių atakų sąvoką. • Išmanyti socialinės inžinerijos ir atvirkštinės socialinės inžinerijos apibrėžimą. • Suprasti socialinės inžinerijos būdus ir jos ryšį su kibernetinėmis atakomis. • Suprasti dažniausiai pasitaikančias kibernetinio saugumo grėsmes. • Suprasti pagrindines kibernetinių atakų kategorijas ir metodus.
Išankstiniai reikalavimai	Pagrindinės IT ir verslo žinios gali būti naudingos, norint geriau suprasti modulį.
Dalyko (modulio) aprašas	Bus siekiama supažindinti studentus su kibernetinėmis atakomis, didelį dėmesį skiriant sukčiavimui (angl. phishing). Taip pat bus nagrinėjama socialinės inžinerijos bei atvirkštinės socialinės inžinerijos pritaikymas kibernetinių išpuolių metu. Dalyke bus nagrinėjami skirtingi sukčiavimo (angl. phishing) atakų tipai ir metodika kartu su pateikiamais realiais pavyzdžiais iš projekte dalyvaujančių partnerių šalių.

<table>
<tr><th colspan="4">DALYKO (MODULIO) TEMOS</th></tr>
<tr><td>3.1</td><td>Kibernetinių atakų įvadas</td><td colspan="2">• Trumpas kibernetinių atakų įvadas skiriant didelį dėmesį sukčiavimui (angl. phishing).</td></tr>
<tr><td colspan="2"></td><td>Rekomenduojama trukmė
30 min.</td><td>Mažiausiai skaidrių
8
Daugiausiai skaidrių
10</td></tr>
<tr><td>3.2</td><td>Socialinės inžinerijos moduliai ir manipuliacija</td><td colspan="2">• Socialinės inžinerijos modelių apžvalga, skiriant didelį dėmesį:
a) R. Cialdini „Įtikinėjimo principai“[1]:
- apsikeitimas (angl. Reciprocation),
- įsipareigojimas ir nuoseklumas (angl. Commitment and consistency),
- priimtinumas (žmonės linkę pritarti daugumos nuomonei, angl. Social proof),
- simpatijoms (žmonės linkę padėti asmenims, kurie jiems patinka angl. Liking),
- valdžia, autoritetas (angl. Authority),
- trūkumas, stygius (žmonės neretai trokšta dalykų, kurių neturi).
b) Socialinės inžinerijos psichologiniai aspektai.
c) Atvirkštinės socialinės inžinerijos apžvalga.</td></tr>
<tr><td colspan="2"></td><td>Rekomenduojama trukmė
4 valandos</td><td>Mažiausiai skaidrių
60
Daugiausiai skaidrių
80</td></tr>
<tr><td>3.3</td><td>Skirtingi sukčiavimo (angl. phishing) atakų tipai ir kategorijos</td><td colspan="2">• Skirtingi kibernetinių atakų, ypač sukčiavimo (angl. phishing), tipai bei kaip juos atpažinti.
Kategorijos:
- su BDAR (Bendruoju duomenų apsaugos reglamentu) susijusios atakos,
- elektroniniai laiškai,
- tiesioginio susirašinėjimo žinutės,
- socialiniai tinklai,
- svetainės,
- netikrų loterijų pranešimai,
- SMS žinutės,
- telefoniniai skambučiai,
- gyvai vykstantys susitikimai,
- duomenų vagystė paslapčia stebint duomenis vedantį asmenį.
Atakų tipai:
- „Spray and pray“ (el. laiškai siekiant pavogti konfidencialią informaciją),
- „Spear phishing“ (personalizuotas sukčiavimas (angl. phishing)),
- „Whaling“ (bandymas pavogti konfidencialią informaciją ir dažnai nukreiptas į aukščiausią vadovybę),
- „Vishing“ (telefoninis sukčiavimas),</td></tr>
</table>

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

<table>
<tr><td></td><td colspan="3">- „Smishinf“ (sukčiavimas SMS žinutėmis),
- „Angler Phishing“ (sukčiavimas socialiniuose tinkluose),
- „Clone Phishing“ (tikrų laiškų turinio panaudojimas sukčiavimui),
- „Malwertising“ (kenkėjiškas turinys reklamose).</td></tr>
<tr><td></td><td>Rekomenduojama trukmė
4 valandos</td><td>Mažiausiai skaidrių
60</td><td>Daugiausiai skaidrių
80</td></tr>
<tr><td>3.4 Konkrečių pavyzdžių nagrinėjimas</td><td colspan="3">• Kelių skirtingų partnerių organizacijų pavyzdžių pristatymas ir nagrinėjimas.
• Kontaktiniu ar nuotoliniu būdu vykstanti diskusija nedidelėse grupėse (sudarytose iš 5-6 studentų).
Pastaba: studentų bus prašoma ne tik diskutuoti, bet ir analizuoti neseniai įvykdytą sukčiavimo (angl. phishing) ataką bei paminėti svarbias detales, tokias kaip atakos data, informacija apie auką, atakos pobūdis, kokios jos pasekmės, išmoktos pamokos ir pan. Po to, grupė išrinks vieną atstovą, kuris pristatys analizės rezultatus visai auditorijai. Tada dėstytojai ir kiti studentai pateiks konstruktyvų grįžtamąjį ryšį.</td></tr>
<tr><td></td><td>Rekomenduojama trukmė
1 val. 30 min.</td><td>Mažiausiai skaidrių
22</td><td>Daugiausiai skaidrių
30</td></tr>
</table>

1.2.4 Kibernetinių atakų atpažinimas ir apsauga

Dalyko (modulio) pavadinimas	4.0 Kibernetinių atakų atpažinimas ir apsauga
Bendra trukmė *(valandomis / skaidrėmis)*	14 valandų 210–255 skaidrės
Mokymo metodai	Kontaktiniu būdu, Nuotoliniu būdu, Mišriuoju būdu.
Įvertinimas	Kontaktiniu būdu ar internetiniu testu.
Dalyko (modulio) siekiniai	• Įgyti pagrindinių žinių apie e. saugą ir saugumas. • Suprasti skirtingą informacijos turinį. • Išmanyti tapatybės apibrėžimą bei gebėti atskirti atakas, nukreiptas prieš asmeninius duomenis. • Suprasti potencialių kibernetinių atakų pasekmes, kurios nukreipiamos prieš individualius asmenis ar/ir tam tikras organizacijas. • Apibrėžti ir suprasti kibernetinės higienos sąvoką bei aptarti jos svarbą gynybos prieš kibernetines atakas procese. • Suprasti ir taikyti įvairius apsaugos nuo kibernetinių atakų metodus. • Gebėti parengti ir pritaikyti kibernetinio incidento valdymo planą.
Išankstiniai reikalavimai	Ankstesni dalykai (moduliai)
Dalyko (modulio) aprašas	Dalyko metu siekiama supažindinti studentus su kibernetinio saugumo sąvoka bei su iniciatyvumo svarba, taikant kibernetinės higienos koncepciją ir siekiant apsisaugoti nuo virtualių atakų. Modulyje taip pat išsamiai aprašoma, kaip atpažinti kibernetines atakas ir kaip su jomis elgtis. Modulis supažindina su reagavimo į incidentus planų kūrimu ir įgyvendinimu, siekiant sumažinti kibernetinių atakų poveikį.

<table>
<tr><th colspan="4">DALYKO (MODULIO) TEMOS</th></tr>
<tr><td>4.1 Pagrindinės žinios apie e. saugumą</td><td colspan="3">

Informacijos turinio skirtumai (laisvai prieinami duomenys, asmeninė, verslo informacija ir kt.); intelektinė nuosavybė; autorių teisės.
Suprasti tapatybės sąvoką; žinoti apie tapatybės vagystę ir vagystės būdus. Žinoti apie šnipinėjimo programas, klaviatūros šnipinėjimą, sukčiavimo strategijomis, kurios naudojamos parduodant prekes, Trojos arklius. Žinoti įvairius būdus, kaip kenkėjiška programinė įranga gali patekti į įrenginį.
Žinoti apie tapatybės ir asmens duomenų vagysčių darbe ir internete priežastis ir pasekmes (apgaulingas informacijos naudojimas, informacijos praradimo grėsmė, tam tikri sąmokslai).
Žinoti apie grėsmes, susijusias su asmens duomenų atskleidimu.
Trumpai supažindinti su kibernetinių atakų poveikiu asmeniui ir organizacijai. Išsamesnė informacija bus nagrinėjama 4.4 skirsnyje.

<table>
<tr><td>Rekomenduojama trukmė
30 min.</td><td>Mažiausiai skaidrių
8</td><td>Daugiausiai skaidrių
10</td></tr>
</table>
</td></tr>
<tr><td>4.2 Prevencinės priemonės</td><td colspan="3">

Kibernetinė higiena internete (kuo mažiau informacijos apie asmenis, įskaitant asmenines paskyras socialinėje žiniasklaidoje, kadangi ši informacija gali tapti sukčių taikiniu).
Kibernetinė higiena darbo vietoje.
Speciali įranga ir technologijos (filtrai ir apgaulingų el. laiškų blokavimas).

<table>
<tr><td>Rekomenduojama trukmė
2 valandos</td><td>Mažiausiai skaidrių
30</td><td>Daugiausiai skaidrių
35</td></tr>
</table>
</td></tr>
<tr><td>4.3 Kibernetinių atakų atpažinimas</td><td colspan="3">

Atvejų analizė pasitelkiant 3.3 skyriuje „Skirtingi sukčiavimo (angl. phishing) atakų tipai ir kategorijos“ aprašytus metodus.
Kibernetinių atakų atpažinimas (atsižvelgiant į ankstesnio skyriaus punktus), įskaitant, bet neapsiribojant:

kritinis mąstymas,
laiške esančios nuorodos tikrinimas jos nepaspaudžiant,
supratimas, kas yra URL,
pranešimų analizė,
pagrindinių požymių (angl. red flags) atpažinimas.

<table>
<tr><td>Rekomenduojama trukmė
5 valandos</td><td>Mažiausiai skaidrių
75</td><td>Daugiausiai skaidrių
90</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><td>4.4</td><td>Kibernetinių atakų valdymas</td><td colspan="3">

Kibernetinio saugumo vadovas, skirtas šios srities žinių gilinimui bei dalis, kurioje aptariama asmenims bei organizacijoms padaryta žala.
Dalis veiksnių, kurie padeda apsisaugoti nuo kibernetinių atakų:
- saugi navigacija,
- patikimi ir „stiprūs“ slaptažodžiai,
- atakų vengimas,
- saugus apsipirkimas internete,
- specialios programos, skirtos kovoti su kibernetinėmis atakomis,
- darbas su slapukais,
- atsarginių duomenų kopijų kūrimas,
- failų šifravimas,
- dviejų veiksnių (žingsnių) autentifikavimas,
- kenkėjiška programinė įranga,
- saugus naršymas.
Lokalių, Europos ir tarptautinių atvejų analizė.
Nuosekliai aptariamas kiekvienas instrukcijos žingsnis bei iliustracijos.
Pateikiami reagavimo į kibernetinę ataką veiksmai, kurių gali imtis nukentėjęs asmuo arba įmonė bei tai, kokių priemonių imtis siekiant atitaisyti žalą.

<table>
<tr><td>Rekomenduojama trukmė
5 valandos</td><td>Mažiausiai skaidrių
75</td><td>Daugiausiai skaidrių
90</td></tr>
</table>
</td></tr>
<tr><td>4.5</td><td>Žalos sumažinimas pasinaudojant incidento valdymo planu</td><td colspan="3">

Sukurti, parengti ir įgyvendinti reagavimo į incidentus planą, kuriame nurodomi siūlomi ir geriausios praktikos metodai, taikytini įvykus duomenų saugumo pažeidimo incidentui.
Pastaba: šią dalį galima pritaikyti priklausomai nuo šalyje taikomų būdų.

<table>
<tr><td>Rekomenduojama trukmė
1 val. 30 min.</td><td>Mažiausiai skaidrių
22</td><td>Daugiausiai skaidrių
30</td></tr>
</table>
</td></tr>
</table>