



Catedra Internațională Onorifică
"Jean BART" în sprijinul Strategiei UE
pentru Regiunea Dunării (CIO-SUERD)



Fundația EUROLINK
Casa Europei

euro.solutions
market



Asociația "Comunitățile Locale
Riverane Dunării" - CLDR
Membră CoDCR



PROGRAMUL NAȚIONAL COMUN DE FORMARE

CURS

INCIDENTE DE SECURITATE

GDPR & CYBERSECURITY

Abordare, Evaluare, Prevenție, Acțiune, Căi de atac

2019

MODULUL 1

CyberSecurity

Autori:

Adriana Huțuțui, Jurist

Ionuț Socol, specialist IT

Sever Avram, Profesor Asociat și Coordonator General al
Catedrei Internaționale Onorifice "Jean Bart"

Sandu Zamfirescu, Formator certificat & Cercetător Asociat Academia Română,
Director Comunicare - Relații Publice al Asociației CLDR România

X. Cuprins	
I. Prezentare inițială	3
II. Definiții și termeni	4
III. CyberSecurity – baze și vulnerabilități	13
Ce este CyberSecurity?	13
De ce avem nevoie de CyberSecurity	13
Identitatea dumneavoastră online și offline	14
Ce este regulamentul privind protecția generală a datelor (GDPR).....	14
Despre datele dumneavoastră.....	15
Unde sunt datele dumneavoastră.....	16
Riscul expunerii neautorizate a datelor dumneavoastră.....	16
Regulamentul de CyberSecurity	17
Obiectivele principale ale Regulamentul de CyberSecurity	22
Securitatea cibernetică în cifre	23
Factorul uman.....	24
Procese	24
Tehnologie.....	25
Importanța securității cibernetică	26
Securitatea informatică este o chestiune critică	26
Pierderile și costurile pentru încălcarea securității datelor	27
Atacurile cibernetică devin din ce în ce mai sofisticate.....	29
Care sunt consecințele unui atac cibernetic?.....	30
Atacurile cibernetică devin mai profitabile.....	31
IV. Elemente de securitate cibernetică	32
Protecția aplicațiilor	32
Securitatea rețelei	32
Securitatea operațională	32
Instruirea utilizatorilor finali	32
Bordul administrativ și implicarea sa.....	33
V. IoT – Internetul lucrurilor	34
Ce este Iot.....	34



CURS

INCIDENTE DE SECURITATE
GDPR & CYBERSECURITY

Cuprins

Câte dispozitive IoT ne înconjoară	36
Securitatea IoT	37
Avantaje și temeri legate de echipamentele IoT	38
VI. Testele de penetrare.....	39
Scopul testelor de penetrare	40
Prezentarea evaluării vulnerabilităților	41
Prezentarea testelor de penetrare.....	41
Tipuri de teste de penetrare	42
Rolul și responsabilitățile echipei de testare	43
Dezavantajele testelor de penetrare.....	43
Cât de des trebuie să efectuați teste de penetrare	44
VII. Atacuri cibernetice și amenințări de securitate	46
Phishingul.....	46
Inginerie sociala	47
DDoS (denial-of-service distribuit) atac	47
Virusii.....	47
Viermi	48
Malware.....	48
Troian	48
Ransomware – răscumparare	48
Spyware / adware	49
Injecție prin SQL.....	49
Atacul de tip MITM (man-in-the-middle).....	50
Vulnerabilități în aplicațiile și rețelele web	50
Atacul de tip Ziua Zero	51
VIII. Analiza atacurilor cibernetice	53
Identificare și recunoaștere	55
Recunoașterea externă	57
Recunoașterea internă.....	65
Atacul efectiv	67
Analiza tendințelor actuale	68



CURS

INCIDENTE DE SECURITATE
GDPR & CYBERSECURITY



Atacurile de extorcare.....	68
Manipularea datelor	69
Atacurile dispozitivelor IoT.....	70
Backdoors	71
Atacurile cu dispozitive mobile	72
Hackingul dispozitivelor de zi cu zi	74
Hackingul cloudurilor.....	75
Phishingul	77
Exploatarea unei vulnerabilități.....	78
Zero-Day.....	79
Fuzzing	79
Analiza codului sursă.....	80
Tipuri de tip Zero-Day.....	80
Buffer overflows.....	81
Analizatorul de excepție structurat suprascrie.....	81
Modul de acțiune și atac	82
Comandă și control	83
Descoperire și răspândire	84
Extracție și exfiltrare	84
IX. Atacuri de tip Ransomware - Răscumpărare.....	87
Evoluția Ransomware în 2018	87
Recomandări generale cu privire la acest tip de atac	88
Despre Maoloo.....	90
Despre Phobos	91
Despre GandCrab.....	92
Despre LockCrypt.....	93
Despre Annabelle.....	93
Despre LooCipher.....	94
Riscuri critice pentru securitatea cibernetică	95
X. Cuprins	98



CURS

INCIDENTE DE SECURITATE
GDPR & CYBERSECURITY





Catedra Internațională Onorifică
"Jean BART" în sprijinul Strategiei UE
pentru Regiunea Dunării (CIO-SUERD)



Fundația EUROLINK
Casa Europei

euro.solutions
market



Asociația "Comunitățile Locale
Riverane Dunării" - CLDR
Membră CoDCR



PROGRAMUL NAȚIONAL COMUN DE FORMARE

CURS

INCIDENTE DE SECURITATE

GDPR & CYBERSECURITY

Abordare, Evaluare, Prevenție, Acțiune, Căi de atac

2019

MODULUL 2

Incidente de securitate GDPR

Autori:

Adriana Huțuțui, Jurist

Ionuț Socol, specialist IT

Sever Avram, Profesor Asociat și Coordonator General al
Catedrei Internaționale Onorifice "Jean Bart"

Sandu Zamfirescu, Formator certificat & Cercetător Asociat Academia Română,
Director Comunicare - Relații Publice al Asociației CLDR România

XII. Cuprins

I. Scurt introducere în GDPR	3
Ce este regulamentul privind protecția generală a datelor (GDPR)?	3
Domeniul de aplicare material	6
Domeniul de aplicare teritorial	7
II. Breșele – incidentele de securitate	8
Probabilitatea apariției unei breșe de securitate	8
Ce este o breșă de securitate	8
Când o breșă devine o încălcare a securității datelor personale	9
Când un incident devine o încălcare a securității datelor personale	9
Tipuri de încălcări ale datelor cu caracter personal	12
Prevenirea apariției unei breșe de securitate	15
Măsuri organizatorice	21
Măsuri tehnice	23
Probarea măsurilor întreprinse	26
Impactul unei breșe de securitate	28
Posibilele consecințe ale încălcării datelor cu caracter personal	30
Când un operator devine "conștient"	32
Ce încălcări trebuie să notificăm autorităților	37
Ce rol au împuterniciții în breșele de securitate	39
În cât timp trebuie să raportăm o încălcare	39
Ce informații trebuie să conțină o notificare de încălcare	40
Dacă nu avem încă toate informațiile necesare	40
Ce se întâmplă dacă nu vom notifica?	41
Cum notificăm o încălcare la autoritatea de supraveghere	42
Când trebuie să anunțăm persoanele vizate despre o încălcare?	42
Măsuri suplimentare impuse de GDPR ca răspuns la o încălcare	44
Ce altceva ar trebui să luăm în considerare?	44
Instruirea și responsabilizarea angajaților	45
Riscurile Angajaților	51
III. Asigurați pentru incidente de securitate	52



CURS

INCIDENTE DE SECURITATE
GDPR & CYBERSECURITY



Situația asigurărilor cibernetice din SUA	52
Situația din Uniunea Europeană	54
Ce va însemna GDPR pentru asigurarea cibernetic ?	55
Asigurarea eventualelor amenzi pentru încălcarea GDPR	57
Asigurare de Răspundere privind Protecția Datelor GDPR & CyberSecurity	60
Asigurarea de Răspundere privind Protecția Datelor GDPR	62
Asigurarea de Răspundere cibernetic CyberSecurity	64
Tabel comparativ Asigurări GDPR & CyberSecurity	65
Condiții generale pentru tipul de Asigurări GDPR & CyberSecurity	66
IV. Investigarea unui incident	70
Detectarea incidentelor	70
Analizarea incidentului	71
Evaluarea riscurilor	71
Activarea Procedurii de Răspuns la Incident	73
Convocarea Echipei de Răspuns la Incident	74
Membrii Echipei de Răspuns la Incident	74
Roluri și responsabilități	75
Agenda standard pentru întâlnirile Echipei de Răspuns la Incident	77
Managementul Incidentului, Monitorizare și Comunicare	78
Procedurile de comunicare	78
Comunicarea cu Autoritatea privind Supravegherea Datelor cu Caracter Personal	79
Comunicarea cu Persoanele vizate	80
Alte comunicări externe	81
Comunicarea cu mass media	81
Măsurile reparatorii	83
Izolare	83
Eradicare	86
Recuperare	87
Notificarea	87



CURS

INCIDENTE DE SECURITATE
GDPR & CYBERSECURITY



Cuprins

Activitatea de după incident	88
Notificarea Autorității de supraveghere (ANSPDCP)	89
Informarea persoanelor vizate cu privire la incidentele de securitate	92
V. Plan supraviețuire în caz de incident de securitate	95
VI. Învățăm din breșele anterioare	96
VII. Evaluarea riscurilor	99
Evaluarea riscului pentru terți – furnizori - împuterniciți	100
VIII. Exemple de breșe și incidente de securitate	102
Exemplu 1 – pierdere echipamente	102
Exemplu 2 – pierdere bază de date	102
Exemplu 3 – pierderea unei copii unice a unei baze de date	102
Exemplu 4 – expunerea datelor angajaților	103
Exemplu 5 – expunerea datelor pacienților	103
Exemplu 6 – expunerea publică a unui fișier de export	103
Exemplu 7 – pierderea unor hard-discuri cu date	104
Exemplu 8 – distrugerea unei baze de date	104
Exemplu 9 – Expunerea datelor din neglijență	104
Exemplu 10 – Expunerea datelor din neglijență	104
Exemplu 11 – liste de evenimente expuse	104
Exemplu 12 – aplicații cu erori de programare 1	105
Exemplu 13 – aplicații cu erori de programare 2	105
Exemplu 14 – transmitere e-mail spre destinatar greșit	105
Exemplu 15 – pierderea corespondenței	105
Exemplu 16 – corespondență cu surprize	106
Exemplu 17 – Chiar mie? Nu, mie nu mi se poate întâmpla ...	106
Exemplu 18 – pericolul vă așteaptă la fiecare colț	106
Exemplu 19 – când breșele de securitate ale lor devin ale noastre	106
Exemplu 20 – un update și datele s-au pierdut?	107
Exemplu 21 – breșe de securitate transmise mai departe	107
Exemplu 22 – atacuri cibernetice și virusii prezenți peste tot	107
IX. Breșe de securitate din ultimul an	109



CURS

INCIDENTE DE SECURITATE
GDPR & CYBERSECURITY



Cuprins

X.	Breșe și incidente de securitate naționale	110
	Un sac cu documente personale descoperit de inspectorii	110
	Datele a mii de români, dezvăluite pe internet	111
	15.000 Euro pentru încălcarea GDPR de către un hotel	111
	Unicredit Bank - 130.000 Euro amenda pentru încălcat GDPR	114
	Avocatoo - 3000 Euro pentru o breșă GDPR	116
XI.	Breșe și incidente de securitate internaționale	121
	WeTransfer – fișierele au fost expediate către alți destinatari	121
	Echipamentele IT din ultimii 10 ani au o vulnerabilitate din fabricație	122
	British Airways – datele a 380.000 clienți au fost furate	123
	Facebook 50 de Milioane de conturi compromise	123
	Google+ a fost închis deoarece a compromis 52,5 de Milioane de conturi	124
	Breșă la Huazhu – China – 100 Milioane de persoane afectate	124
	Breșă majoră în securitatea iPhone	125
	Breșă Huawei anunțată de Vodafone	125
	Breșă de la NSA - USA	126
	Breșă de la Marriott International – 339 Milioane de clienți	127
	Baza de date cu 763 Milioane de adrese unice de e-mail	127
	Peste 770 Milioane de adrese e-mail și 21 Milioane de parole compromise	128
XII.	Cuprins	129



CURS

INCIDENTE DE SECURITATE
GDPR & CYBERSECURITY





Catedra Internațională Onorifică
"Jean BART" în sprijinul Strategiei UE
pentru Regiunea Dunării (CIO-SUERD)



Fundația EUROLINK
Casa Europei

euro.solutions
market



Asociația "Comunitățile Locale
Riverane Dunării" - CLDR
Membră CoDCR



PROGRAMUL NAȚIONAL COMUN DE FORMARE

CURS

INCIDENTE DE SECURITATE GDPR & CYBERSECURITY

Abordare, Evaluare, Prevenție, Acțiune, Căi de atac

2019

MODULUL 3

Autorități pentru aplicarea GDPR & CyberSecurity

Autori:

Adriana Huțuțui, Jurist

Ionuț Socol, specialist IT

Sever Avram, Profesor Asociat și Coordonator General al
Catedrei Internaționale Onorifice "Jean Bart"

Sandu Zamfirescu, Formator certificat & Cercetător Asociat Academia Română,
Director Comunicare - Relații Publice al Asociației CLDR România

XII. Cuprins

I. Prezentare inițial	3
II. CyberSecurity la nivelul Uniunii Europene	4
Directiva NIS – Directiva EU 1148/2016	4
Cronologie CyberSecurity la nivel european	7
Statistici CyberSecurity	9
ENISA - Agenția a Uniunii Europene pentru Securitatea Rețelelor și a Informațiilor	10
Cum funcționează ENISA	11
CSIRT	12
Serviciile CSIRT	13
CSIRT-uri active la nivel european	14
CyberSOPex2019	15
CERT-EU	16
Securitatea cibernetică în sectorul energetic	17
Recomandări video EINSIA – în limba engleză	20
III. CyberSecurity la nivel Național	21
Autorități competente la nivel național	24
Principiile care stau la baza Legii NIS	25
1. Principiul responsabilității și conștientizării	25
2. Principiul proporționalității	25
3. Principiul cooperării și coordonării	25
Domeniile de aplicare ale acestei legi	25
Operatorii de servicii esențiale	25
Obligațiile operatorilor de servicii esențiale	28
Ce trebuie să pună la dispoziție operatorii la solicitare CERT-RO	29
Coordonarea strategică la nivel național	30
Echipele de intervenție în caz de incidente de securitate informatică	31
Autoritatea competentă la nivel național - CERT-RO	32
Care sunt atribuțiile generale ale CERT-RO ca autoritate competentă la nivel național	32



CURS

INCIDENTE DE SECURITATE
GDPR & CYBERSECURITY



Atribuții CERT-RO în calitate de punct național unic de contact.....	36
Atribuții CERT-RO în calitate de CSIRT național.....	37
Asigurarea securității rețelelor și sistemelor informatice	39
Care sunt cerințele minime de securitate?	39
Notificarea incidentelor de securitate.....	41
Ce informații trebuie să conțină în mod obligatoriu notificarea incidentelor de securitate.....	41
Managementul notificărilor - incidentelor de securitate	43
IV. Protecția datelor personale la nivel European.....	45
AEPD - EDPS - Autoritatea Europeană pentru Protecția Datelor	45
CEPD - EDPB - Comitetul European pentru Protecția Datelor	46
Autorități de supraveghere la nivelul fiecărui stat european.....	47
V. Protecția datelor personale la nivel Național	54
Despre ANSPDCP – Autoritatea Națională Privind Protecția Datelor cu Caracter Personal	54
Depunerea petițiilor din partea persoanelor fizice	56
Declarare persoană desemnată DPO	57
Raportare breșe și incidente de securitate	57
Raportare breșe și comunicații electronice	58
Plata amenzilor	60
VI. Pregătirea organizației pentru investigațiile GDPR.....	62
Verificări și pregătiri prealabile	62
În ce condiții puteți fi subiectul unei investigații din partea ANSPDCP ...	65
Soluționarea unei petiții.....	65
Desfășurarea unei investigații tematice sau din oficiu	66
Verificarea site-urilor web.....	68
Recomandări suplimentare.....	69
VII. Investigații GDPR din partea autorităților	71
Despre investigațiile GDPR	71
Diferențe între tipurile de investigații	73
Cine poate desfășura o investigație GDPR	75



CURS

INCIDENTE DE SECURITATE
GDPR & CYBERSECURITY



Exercitarea atribuțiilor autorităților.....	75
Instrumente și opțiuni ale autorităților.....	77
Descurajarea neconformității și încălcării GDPR.....	78
Efectuarea investigațiilor GDPR pe teren.....	80
Activitățile inspectorilor în investigațiile din teren.....	83
Efectuarea investigațiilor GDPR la sediul autorității.....	85
Efectuarea investigațiilor GDPR în scris.....	87
Efectuarea investigațiilor autorităților publice.....	88
Drepturi și obligațiile operatorului investigat.....	90
Drepturile operatorului investigat.....	90
Obligațiile operatorului investigat.....	90
Obstrucționarea investigațiilor sau inspectorilor.....	91
Procesul verbal de constatare sancționare întocmit la finalizarea investigației.....	92
Măsurile corective, plan de remediere.....	94
Sanțiuni transpuse în amendă.....	97
Amenzile prevăzute în Regulamentul European 679/2016.....	98
Amenzile prevăzute în Legea 190/2018.....	103
Amenda cu valoare de titlu executoriu.....	108
Sanțiuni din partea persoanelor vizate.....	108
Modul de stabilire a cuantumului amenzilor.....	108
Timpul de răspuns la solicitările ANSPDCP.....	111
VIII. Notificări brevie și răspunsuri la solicitările autorităților.....	113
Ce informații trebuie să conțină o notificare de încălcare a autorității de supraveghere?.....	114
Dacă nu avem încă toate informațiile necesare?.....	114
Cum putem notifica o încălcare ANSPDCP?.....	115
Ce se întâmplă dacă nu vom notifica?.....	116
Când trebuie să anunțăm persoanele vizate despre o încălcare?.....	117
GDPR ne obligă să luăm orice altă măsură în răspuns la o încălcare?....	118
Ce altceva ar trebui să luăm în considerare?.....	119



CURS

INCIDENTE DE SECURITATE
GDPR & CYBERSECURITY



R spunsul la solicitările autorității de supraveghere.....	120
IX. Contestății, termene de prescripție, c i de atac	124
Termene de contestare i atac	125
Persoanele fizice.....	126
Recomandări privind contestarea	127
Termene de prescripție	129
X. Sancțiuni GDPR aplicate.....	130
Sancțiuni aplicate la nivelul României.....	130
ANSPDCP a amendat un operator de date personale cu 15.000 Euro pentru încălcarea prevederilor GDPR	130
Avocatoo - 3000 Euro pentru o bre GDPR	134
Astfel, Autoritatea de supraveghere a decis sancționarea operatorului bancar cu amenda contravențional pentru ca a încălcat prevederile impuse prin Regulamentul 679/2016 GDPR și a drepturilor persoanelor vizatePrimăria CLUJ sancționat de către ANSPDCP.....	138
ANSPDCP a amendat un operator de date personale 200.000 lei pentru nerespectarea GDPR în privința unui incident de securitate	139
ANSPDCP sancționează cel mai mare operator de telecomunicații pentru prelucrare nelegală a datelor clienților	139
ANSPDCP sancționează un operator de telecomunicații și tearg datele cu caracter personal colectate fără avizul clienților.....	139
ANSPDCP amendează cu 7.000 lei un operator de telefonie, catv și acces internet pentru că încălce GDPR	140
ANSPDCP sancționează un operator de telefonie pentru comunicări comerciale fără consimțământ	140
ANSPDCP sancționează cu amenda un Centru medical – 10.000 lei..	140
Cea mai mare amenda GDPR la nivel național: Unicredit Bank 130.000 Euro pentru nerespectarea prevederilor GDPR	143
Sancțiuni aplicate la nivelul Uniunii Europene.....	145
Angajat service auto condamnat la 6 luni închisoare cu executare	145
Încălcarea dreptului la intimitate a chiriei	146
Amenzi după investigațiile a 40 de site-uri web.....	148
Ofițer de poliție sancționat cu amenda de 1.400 Euro.....	149



CURS

INCIDENTE DE SECURITATE
GDPR & CYBERSECURITY

Primar din Belgia sancționat cu amenda de 2.000 Euro.....	150
Monitorizare CCTV 6 angajati i nerespectare m suri impuse – 20.000 euro	151
Site web - date personale expuse - 20.000 Euro.....	152
Partid politic ungar – bre de securitate – 35.000 Euro	153
Apeluri nesolicitate marketing direct – 80.000 Lire.....	155
Apeluri in scop de de marketing f r consimț mânt – 90.000 Lire	155
Între 10 februarie 2017 i 24 septembrie 2018 Smart Home Protection Ltd a utilizat un serviciu public de telecomunicații în scopul efectu rii a 125 de solicit ri nesolicitate de marketing direct c tre abonați, în cazul în care num rul alocat abonatului pentru linia numit a fost un num r enumerat pe registrul numerelor p strate de comisar în conformitate cu regula 26, contrar dispozițiilor articolului 21 alineatul (1) litera (b) din PECR; i	156
De asemenea, comisarul este mulțumit în sensul regulamentului 21 c aceste apeluri au fost adresate abonaților care s-au înregistrat la TPS cu cel puțin 28 de zile înainte de primirea apelurilor i nu i-au dat acordul prealabil pentru Smart Home Protection Ltd pentru a primi apeluri....	156
Mesaje SMS in scop de de marketing f r consimț mânt – 100.000 Lire	157
Pierderea unui stick cu date personale - 120.000 Lire.....	157
Apeluri telefonice nesolicitate – 250.000 Lire	161
Nerespectarea termenelor de stergere a datelor – 200.000 Euro	162
Spitalul Barreiro – amendat cu 400.000 Euro	163
Uber – date expuse într-un atac cibernetic– 385.000 Lire.....	163
Spitalul Haga – amendat cu 460.000 Euro	165
Vulnerabilitate in site web - 400.000 Euro.....	165
Schimb de date personale – 400.000 Lire.....	167
Facebook - 500.000 Lire pentru o bre a de securitate.....	168
Google – 50 Milioane Euro	169
Cea mai mare amenda GDPR la nivel internațional: 183.390.000 Lire pentru British Airways	172
XI. Cadru legislativ	174
Legislația european	174



CURS

INCIDENTE DE SECURITATE
GDPR & CYBERSECURITY

Cuprins

Legislatia nationala	174
Decizii interne ANSPDCP	176
Decizii interne ANSPDCP abrogate	177
XII. Cuprins	180



CURS

INCIDENTE DE SECURITATE
GDPR & CYBERSECURITY





Catedra Internațională Onorifică
"Jean BART" în sprijinul Strategiei UE
pentru Regiunea Dunării (CIO-SUERD)



Fundația EUROLINK
Casa Europei

euro.solutions
market



Asociația "Comunitățile Locale
Riverane Dunării" - CLDR
Membră CoDCR



PROGRAMUL NAȚIONAL COMUN DE FORMARE

CURS

INCIDENTE DE SECURITATE

GDPR & CYBERSECURITY

Abordare, Evaluare, Prevenție, Acțiune, Căi de atac

2019

MODULUL 4

Laborator – programe și documente
practice și tehnice

Autori:

Adriana Huțuțui, jurist

Ionuț Socol, specialist IT

Sever Avram, Profesor Asociat și Coordonator General al
Catedrei Internaționale Onorifice "Jean Bart"

Sandu Zamfirescu, Formator certificat & Cercetător Asociat Academia Română,
Director Comunicare - Relații Publice al Asociației CLDR România

XII. Conținut

I. Prezentare inițială	3
II. Politica de gestionare DSAR.....	4
A. Cererea DSAR.....	4
B. Verificare identitatii solicitantului.....	4
C. Informatii privind cererea de acces pentru persoana vizata	4
D. Validarea DSAR.....	5
E. Costuri.....	5
F. Revizuirea informatiilor.....	6
G. Raspunsul la cererile de acces	6
H. Mod de lucru	7
I. Arhivarea	7
J. Diagrama DSAR.....	8
III. Politica de gestionare bre e de securitate.....	9
A. Obiective	9
B. Detectarea incidentelor, evaluarea si analiza acestora	9
C. Activarea Procedurii de Raspuns la Incident.....	12
D. Convocarea Echipei de Raspuns la Incident	13
1. Membrii Echipei de Raspuns la Incident.....	13
2. Roluri si responsabilitati	14
3. Agenda standard pentru intalnirile Echipei de Raspuns la Incident... ..	16
E. Managementul Incidentului, Monitorizare si Comunicare.....	17
F. Procedurile de comunicare.....	17
1. Comunicarea cu Autoritatea privind Supravegherea Datelor cu Caracter Personal.....	18
2. Comunicarea cu Persoanele vizate	18
3. Alte comunicari externe.....	18
4. Comunicarea cu media	19
G. Masuri reparatorii	20
1. Izolare	20
2. Eradicare	22



CURS

INCIDENTE DE SECURITATE
GDPR & CYBERSECURITY



3. Recuperare	22
4. Notificarea	23
H. Activitatea de dupa incident	23
I. Notificarea Autoritatii de supraveghere (ANSPDCP)	24
J. Informarea persoanelor vizate cu privire la incidentele de securitate	26
K. Revizuirea procedurii	28
L. Activitati post incident.....	28
M. Finalizarea procedurii	28
IV. Plan de remediere	30
V. Anunțarea unui incident de securitate GDPR	33
VI. Măsuri tehnice și organizatorice recomandate pentru operatori	40
Gama standard de măsuri tehnice și organizatorice.....	41
Măsuri organizatorice de securitate	41
Măsuri tehnice de securitate	42
Măsuri de asigurare a confidențialității	45
Măsuri de asigurare a integrității	46
Măsuri de asigurare a disponibilității și durabilității.....	46
Măsuri pentru pseudo-anonimizarea datelor cu caracter personal	47
Măsuri pentru criptarea datelor cu caracter personal.....	47
Măsuri pentru restaurarea rapidă a disponibilității datelor după un incident	47
Analiză, evaluare și revizuire periodice	48
Cerințele legislative clare pentru adoptarea de măsuri tehnice și organizatorice.....	49
VII. Liste de verificare pentru CyberSecurity	52
Realizarea de liste de verificare personalizate de CyberSecurity	52
Riscul de atac / Impactul atacului.....	53
Cauze posibile.....	54
Existența atacurilor interne.....	54
Bugetul pentru IT.....	55
Costul pentru departamentele non-IT	55



CURS

INCIDENTE DE SECURITATE
GDPR & CYBERSECURITY



Bugetarea pentru securitatea cibernetic	56
Exemple de check-list de CyberSecurity	57
Exemplul #1	57
Exemplul #2	61
VIII. Instrumente si solutii informatice de preventive si tratament incidente si atacuri cibernetic	74
Solutii de criptare a hard disk-urilor	74
GravityZone Full-Disk Encryption ferit de BitDefender	74
Laboratorul virtual. Cum poate un hacker sa ne fure parolele oferit de SRI	74
Test de Securitate a echipamentului oferit de Quartz Matrix	75
Instrumente anti ransome	76
Decriptor pentru GandCrab	77
Decriptor pentru LockCrypt	77
Decriptor pentru Annabelle	78
Decriptor pentru BTCWare	79
Bitdefender Ransomware Recognition Tool	80
Solutii de imunizare pentru CryptoWall.....	80
Imunizatorul USB	81
Scanner client din reseaua de WIFI pentru acasa	82
Bitdefender Rootkit Remover.....	82
Decriptor LooChiper.....	83
NOMORERANSOM.....	84
Harti live cu amenintari si atacuri cibernetic.....	84
Solutii de scanare si testare vulnerabilitati.....	85
Nmap & Zenmap	85
Metasploit	86
John Ripper	86
THC Hydra	87
Wireshark.....	87
Aircrack-ng	88



CURS

INCIDENTE DE SECURITATE
GDPR & CYBERSECURITY



Nikto	88
Kismet.....	89
Cain i Abel	89
Prismdump.....	90
Tcpdump	90
Scanrand	90
Nessus	91
Penetrarea in servere cu Jenkins	92
IX. Studii de caz – jursiprudență protecția datelor.....	93
1. Raportarea datelor personale c tre sisteme de evidență tip birou de credit	95
FI DE CAZ 1	95
FI DE CAZ 2	96
FI DE CAZ 3	97
2. Prelucrarea datelor personale prin mijloace de supraveghere video.....	97
FI DE CAZ 1	97
FI DE CAZ 2	98
FI DE CAZ 3	99
FI DE CAZ 4	100
FI DE CAZ 5	100
3. Dezv luirea datelor personale c tre diverse entit ți	101
FI DE CAZ 1	101
FI DE CAZ 2	102
FI DE CAZ 3	102
4. Prelucrarea excesiv a datelor personale.....	103
FI DE CAZ 1	103
FI DE CAZ 2	105
FI DE CAZ 3	106
FI DE CAZ 4	106
5. Nerespectarea drepturilor de informare, acces, intervenție și opoziție	107
FI DE CAZ 1	107



CURS

INCIDENTE DE SECURITATE
GDPR & CYBERSECURITY



Cuprins

FI DE CAZ 2	108
FI DE CAZ 3	109
FI DE CAZ 4	110
FI DE CAZ 5	110
6. Transmiterea de comunic ri comerciale prin mijloace de comunica ie electronic	111
FI DE CAZ 1	111
FI DE CAZ 2	112
FI DE CAZ 3	113
7. Înc lcarea regulilor de confiden ialitate și securitate a prelucrărilor de date	114
FI DE CAZ 1	116
FI DE CAZ 2	117
X. Continuitate i Evaluare	119
XI. Cuprins	120



CURS

INCIDENTE DE SECURITATE
GDPR & CYBERSECURITY

